DOI: 10.26354/bb.3.4.101.2025

Patryk Król*
ORCID: 0000-0003-4079-8849
patkro12@gmail.com

Analiza bibliometryczna phishingu

Streszczenie

Cel badania: Artykuł przedstawia kompleksową analizę bibliometryczną literatury naukowej dotyczącej phishingu, ze szczególnym uwzględnieniem sektora bankowego i finansowego, mającą na celu identyfikację kluczowych trendów badawczych, wpływowych autorów oraz perspektywicznych kierunków rozwoju w latach 2003–2024.

Metodologia: Badanie wykorzystuje narzędzie bibliometrix oraz dane z bazy Web of Science obejmujące 4245 dokumentów z 2355 źródeł. Analiza charakteryzuje się roczną stopą wzrostu publikacji wynoszącą 16,35% przy średniej liczbie cytowań 13,73 na dokument. Korpus zawiera publikacje 11 755 autorów z 91 018 referencjami, odzwierciedlając multidyscyplinarny charakter badanej dziedziny.

Wyniki: IEEE Access dominuje z 135 publikacjami, podczas gdy Computers & Security zajmuje drugą pozycję ze 104 publikacjami. Carnegie Mellon University przewodzi wśród instytucji z 75 publikacjami. Analiza ujawnia ewolucję od tradycyjnych metod obrony (2006–2015) w kierunku sztucznej inteligencji i technologii blockchain (2020–2024). Najczęściej cytowanymi publikacjami są prace Jagatic i in. (2007) – 540 cytowań oraz Anderson (2006) – 385 cytowań. Identyfikacja dwóch głównych klastrów tematycznych wskazuje na dychotomię między badaniami nad bezpieczeństwem a metodami wykrywania opartymi na modelowaniu.

Wnioski: Badania nad phishingiem w sektorze finansowym charakteryzują się intensywnym rozwojem z przesunięciem paradygmatu w kierunku personalizowanych systemów wykrywania wykorzystujących uczenie maszynowe. Przyszłe kierunki obejmują interdyscyplinarne badania łączące aspekty techniczne z behawioralnymi oraz zastosowanie technologii blockchain w systemach weryfikacji tożsamości.

Słowa kluczowe: phishing, phishingcyberbezpieczeństwo, sektor bankowy, analiza bibliometryczna, uczenie maszynowe, blockchain, bezpieczeństwo finansowe

Kody JEL: G21, G28, O33, C80

* Patryk Król – Uniwersytet Ekonomiczny w Poznaniu.

Bibliometric Analysis of Phishing

Abstract

Purpose: This article presents a comprehensive bibliometric analysis of scientific literature on phishing with particular emphasis on the banking and financial sector, aiming to identify key research trends, influential authors, and prospective development directions in the period 2003–2024.

Methodology: The study employs the bibliometrix tool and Web of Science database data comprising 4,245 documents from 2,355 sources. The analysis is characterized by an annual publication growth rate of 16.35% with an average of 13.73 citations per document. The corpus contains publications by 11,755 authors with 91,018 references, reflecting the multidisciplinary nature of the research field.

Results: IEEE Access dominates with 135 publications, while Computers & Security ranks second with 104 publications. Carnegie Mellon University leads among institutions with 75 publications. The analysis reveals evolution from traditional defense methods (2006–2015) toward artificial intelligence and blockchain technologies (2020–2024). The most frequently cited publications are works by Jagatic et al. (2007) – 540 citations and Anderson (2006) – 385 citations. Identification of two main thematic clusters indicates a dichotomy between security research and detection methods based on modeling.

Conclusions: Phishing research in the financial sector is characterized by intensive development with a paradigm shift toward personalized detection systems utilizing machine learning. Future directions include interdisciplinary research combining technical with behavioral aspects and application of blockchain technology in identity verification systems.

Keywords: phishing, cybersecurity, banking sector, bibliometric analysis, machine learning, learningblockchain, financial security

JEL Codes: G21, G28, O33, C80

Wstęp

Phishing jako forma cyberprzestępstwa stanowi jedno z najpoważniejszych zagrożeń dla współczesnej gospodarki cyfrowej, w tym sektora finansowego, a zwłaszcza bankowego (Zhuo i in. 2023). Ataki phishingowe, z wykorzystywaniem technik inżynierii społecznej w celu wyłudzenia poufnych informacji, jak dane uwierzytelniające czy informacje finansowe, przybierają coraz bardziej wyrafinowane formy i stanowią istotne wyzwanie dla bezpieczeństwa instytucji finansowych (Yuspin i in. 2024; Mwavali 2024).

W ostatnich latach obserwuje się zarówno gwałtowny wzrost liczby ataków phishingowych, jak i ich zaawansowania technologicznego, co pociąga za sobą z jednej strony przeciwdziałania instytucji odpowiedzialnych za bezpieczeństwo obrotu elektronicznego, jak i osób badających tę problematykę (Do i in. 2022). Według Villanueva i in. (2024) najnowszych danych, od 2018 r. ataki phishingowe wzrosły o 46%, a sektor finansowy ponosi średniorocznie straty w wysokości 3,66 milio-

na dolarów (Villanueva, Sebastian, Dextre 2024). Dane statystyczne wskazują, że około 1,2% wszystkich otrzymywanych wiadomości e-mail to próby phishingu, co przekłada się na 3,4 miliarda phishingowych wiadomości e-mail dziennie, przy czym szacuje się, że jeden na 4200 e-maili stanowi próbę ataku phishingowego (Bhatt i in. 2024).

Ze względu na wysoką wartość transakcji w obrocie elektronicznym sektor finansowy jest szczególnie narażony na skutki ataków phishingowych (Nwafor i in. 2024). Instytucje finansowe muszą borykać się nie tylko z tradycyjnymi, ale także z nowymi formami phishingu, jak: spear phishing, vishing czy ataki wykorzystujące sztuczną inteligencję (Król 2024). Rozwój komunikacji elektronicznej od czasów pandemii COVID-19 dodatkowo zintensyfikował te zagrożenia, przyczyniając się do prawie dwukrotnego wzrostu cyberataków skierowanych przeciwko instytucjom finansowym (Abdajabar, Idbeaa 2024).

Od stosunkowo niedawna analiza bibliometryczna stanowi popularne narzędzie analizy zakresu i struktury badań naukowych w określonej dziedzinie (Donthu i in. 2021). W kontekście badań nad phishingiem tego typu analiza pozwala na systematyczne mapowanie badań, identyfikację kształtujących się trendów, popularnych autorów i instytucji. Zaś analiza metodologiczna takich wyników pozwala na określenie luk w dotychczasowej wiedzy (Mutlutürk i in. 2024). Takie analizy bibliometryczne znajdują zastosowanie także do badania phishingu w sektorze finansowym. Natomiast wyniki tych analiz ułatwiają określenie zarówno tego co zostało już zbadane, jak i wskazanie wyzwań związanych z phishingiem w tym sektorze.

Dotychczasowe badania bibliometryczne w obszarze cyberbezpieczeństwa koncentrowały się głównie na ogólnych aspektach zagrożeń (Perwej i in. 2021). Natomiast stosunkowo niewiele uwagi poświęcono szczegółowej analizie literatury dotyczącej phishingu w sektorze finansowym. Najnowsze analizy wskazują na wzrost zainteresowania badaczy czynnikami psychologicznymi wpływającymi na podatność na phishing, aspektami bezpieczeństwa komunikacji elektronicznej oraz integracją rozwiązań technologicznych z zachowaniami ludzi (Mutluturk, Metin 2023). Ponadto rośnie znaczenie problematyki wykorzystania sztucznej inteligencji i w wykrywaniu i przeciwdziałaniu atakom phishingowym (Olowu i in. 2024).

Celem artykułu jest przeprowadzenie analizy bibliometrycznej literatury naukowej dotyczącej phishingu, ze szczególnym uwzględnieniem sektora finansowego. Analiza obejmuje identyfikację głównych trendów badawczych, mapowanie współpracy międzynarodowej i międzyinstytucjonalnej, określenie najbardziej popularnych publikacji i autorów oraz wskazanie perspektywicznych kierunków przyszłych badań. Zastosowanie zaawansowanych technik bibliometrycznych pozwala na opracowanie kompleksowego obrazu stanu wiedzy w tej dziedzinie oraz wskazanie obszarów wymagających dalszego pogłębienia badań naukowych. Oryginalność opracowania polega na ukierunkowaniu analiz literatury na sektor finansowy, podczas gdy dotychczasowe analizy bibliometryczne phishingu koncentrowały się w większości na ogólnych aspektach cyberbezpieczeństwa.

1. Metodyka badania i ilościowa charakterystyka analizowanych publikacji

W badaniu wykorzystań bibliometrix (Aria, Cuccurullo 2017) oraz dane z bazy Web of Science Core Collection, obejmujące 4245 dokumentów z lat 2003–2024, pochodzące z 2355 źródeł. Frazą wyszukiwania był „phishing". Pozwoliło to na uwzględnienie interdyscyplinarnego przekroju opracowań dotyczących omawianego zagadnienia. Najczęściej cytowane publikacje dotyczące dyscyplin ekonomia i finanse zostały omówione w osobnym fragmencie. Utworzona baza danych odzwierciedla dynamiczny wzrost publikacji z roczną stopą wynoszącą 16,35%, co wskazuje na intensywny rozwój badanej dyscypliny. Średni wiek badanych publikacji wynosi 6,45 lat, łączna liczba referencji 91 018, przy średniej liczbie cytowań na dokument wynoszącej 13,73, co można interpretować jako znaczący wpływ publikacji na środowisko naukowe.

Analiza zawartości dokumentów ujawnia bogactwo wykorzystywanej terminologii naukowej, zidentyfikowano bowiem 1349 słów kluczowych (Keywords Plus) oraz 7975 słów kluczowych autorskich (Author's Keywords). Ta różnorodność terminologiczna odzwierciedla m.in. multidyscyplinarny charakter badanych publikacji, a pośrednio także złożoność poruszanych zagadnień.

Analizą objęto publikacje 11 755 autorów, z których tylko 284 to autorzy publikacji jednoautorskich, co świadczy o wysokim poziomie współpracy autorów. Średnia liczba współautorów na dokument wynosi 3,71. A poziom internacjonalizacji współpracy w badanych dokumentach sięga ca 21%.

W analizowanym zbiorze publikacji dominują materiały konferencyjne (2252 dokumenty, tj. 53,1% ogółu dokumentów), na drugim miejscu są artykuły naukowe (1735, tj. 40,9% całości rekordów) (korpusu). Pozostałe publikacje obejmują przeglądy literatury (94 dokumenty), recenzje książek (17), materiały edytorskie (26) oraz inne nieliczne pozycje. Struktura badanego zbioru dokumentów odzwierciedla ogólną strukturę publikacji we współczesnej nauce, z kapitalną rolą komunikacji konferencyjnej w popularyzacji wyników badań.

2. Wyniki analizy publikacji

Tabela 1 ilustruje liczbę publikacji naukowych dotyczących phishingu według dziesięciu tytułów czasopism naukowych dotyczących phishingu, stanowiąc kluczowy element analizy bibliometrycznej w tym obszarze badawczym.

Tabela 2 przedstawia zestawienie najaktywniejszych autorów publikacji naukowych dotyczących phishingu, uwzględniając całkowitą liczbę prac naukowych. Dane pozwalają zidentyfikować kluczowych naukowców kształtujących krajobraz badań nad phishingiem oraz skalę ich wkładu naukowego.

Tabela 1. Czasopisma naukowe z największą liczbą publikacji dotyczących phishingu indeksowanych w bazie WoS

Lp.	Czasopismo	Liczba publikacji
1.	IEEE Access	135
2.	Computers i Security	104
3.	International Journal of Advanced Computer Science and Applications	51
4.	Electronics	41
5.	Applied Sciences-Basel	34
6.	Expert Systems with Applications	30
7.	International Journal of Computer Science and Network Security	27
8.	Information and Computer Security	22
9.	Security and Communication Networks	22
10.	CMC-Computers Materials i Continua	21

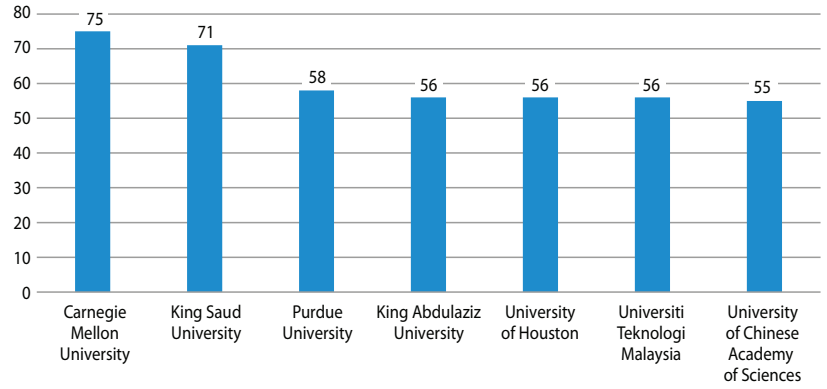
Źródło: opracowanie własne na podstawie danych z bazy WoS, sporządzone za pomocą narzędzia bibliometrix.

Tabela 2. Autorzy z największą liczbą publikacji dotyczących phishingu indeksowanych w bazie WoS

Lp.	Autor	Liczba artykułów
1.	Jain Ankit Kumar	17
2.	Thabtah Fadi	17
3.	Rao Routhu Srinivasa	15
4.	Volkamer Melanie	15
5.	Moore Tyler	14
6.	Varshney Gaurav	14
7.	Allodi Luca	13
8.	Chiba Daiki	13
9.	Chiew Kang Leng	13
10.	Jourdan Guy-Vincent	13
11.	Verma Rakesh M	13
12.	Vishwanath Arun	13
13.	Wu Jiajing	13

Źródło: opracowanie własne na podstawie danych z bazy WoS, sporządzone za pomocą narzędzia bibliometrix.

Rysunek 1. Afiliacje autorów według liczby publikacji dotyczących phishingu indeksowanych w bazie WoS



Źródło: opracowanie własne na podstawie danych z bazy WoS, sporządzone za pomocą narzędzia bibliometrix.

Rysunek 1 przedstawia liczbę publikacji naukowych dotyczących phishingu według afiliacji autorów w siedmiu instytucjach akademickich. Na czele sytuuje się Carnegie Mellon University wyprzedzając o cztery publikacje King Saud University. Pozostałe pięć instytucji ma podobną liczbę publikacji w zakresie od 58 do 55. Warto podkreślić, że z 55 publikacjami znalazł się Uniwersytet Chińskiej Akademii Nauk. Dane rysunku 1 wskazują na globalny charakter badań i publikacji nad phishingiem.

Analiza najczęściej cytowanych publikacji w obszarze badań nad phishingiem ujawnia kluczowe prace, które ukształtowały współczesne rozumienie tego zjawiska. Tabela 3 przedstawia 10 najczęściej cytowanych publikacji w ogólnym zbiorze literatury dotyczącej phishingu, bez rozróżnienia na kategorie tematyczne.

Jagatic i in. (2007) w swoim przełomowym artykule opublikowanym w „Communications of the ACM" zapoczątkowali badania nad social phishingiem. Dotyczyła ona koncepcji wykorzystania sieci społecznych w atakach phishingowych i stworzyła podwaliny pod określenie roli czynników społecznych na podatność osób użytkujących te sieci na ataki. Anderson i Moore (2006) w prestiżowym czasopiśmie „Science" przedstawili fundamentalne analizy ekonomiki bezpieczeństwa, które stały się podstawą do późniejszych badań nad ekonomicznymi aspektami cyberprzestępczości. Praca ta, z 385 cytowaniami WoS, oraz ponad 1100 cytowaniami Google Scholar, wpłynęła na rozwój interdyscyplinarnego podejścia do badań nad phishingiem, łączącego aspekty techniczne z ekonomicznymi. Sheng i in. (2010) w materiałach z konferencji CHI zaprezentowali znaczące badania nad czynnikami wpływającymi na podatność użytkowników na phishing, osiągając 366 cytowań. Ich badania przyczyniły się do lepszego zrozumienie psychologicznych prawidłowości wykorzystywanych przez cyberprzestępców. Xiang i in. (2011) w „ACM Transactions on Information and System Security" przedstawili innowacyjne podejście do wykrywania phishingu, które ma 321 cytowań. Ich metodologia stała się podstawą dla wielu późniejszych

systemów wykrywania ataków phishingowych. Istotna jest także praca Sahingoz i in. (2019) opublikowana w „Expert Systems with Applications", która osiągnęła już 319 cytowań i najwyższą liczbę cytowań rocznie (45,57). Ta publikacja koncentruje się na zastosowaniu sztucznej inteligencji w wykrywaniu phishingu. Krombholz i in. (2015) w „Journal of Information Security and Applications" przeprowadzili kompleksową analizę ataków socjotechnicznych, która była cytowana 291 razy. Ich badania przyczyniły się zarówno do lepszego zrozumienia psychologicznych aspektów phishingu, jak i mechanizmów manipulacji używanych przez atakujących. Khonji i in. (2013) opublikowali w IEEE Communications Surveys i Tutorials ważny przegląd literatury dotyczący phishingu, który osiągnął 266 cytowań, systematyzujący wcześniejsze badania oraz określający kierunki przyszłych prac badawczych.

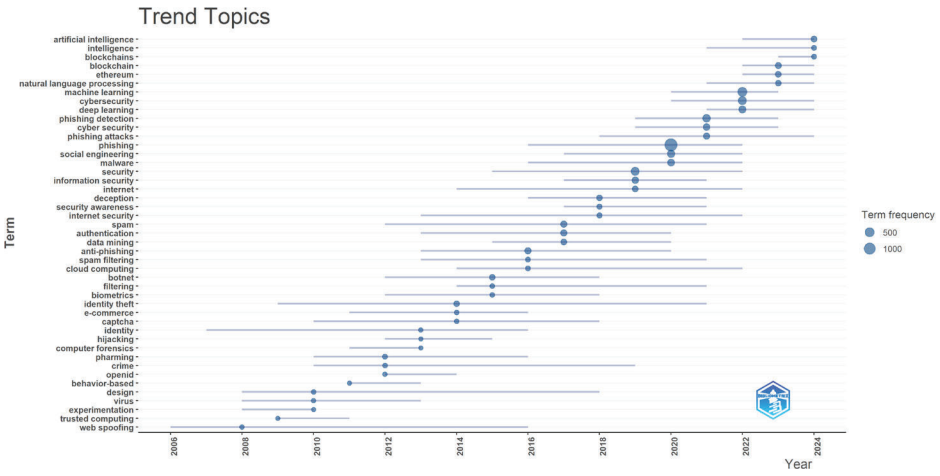
Tabela 3. Autorzy z najczęściej cytowanymi publikacjami dotyczącymi phishingu indeksowanych w bazie WoS

Autor i rok wydania	Czasopismo/Konferencja	Cytowania łącznie	Cytowania rocznie	Cytowania znormalizowane[a)]
Jagatic i in. (2007)	Communications of the ACM	540	28.42	16.63
Anderson i Moore (2006)	Science	385	19.25	17.25
Sheng i in. (2010)	CHI Conference Proceedings	366	22.88	10.67
Xiang i in. (2011)	ACM Transactions on Information and System Security	321	21.40	11.05
Sahingoz i in. (2019)	Expert Systems with Applications	319	45.57	17.67
Krombholz i in. (2015)	Journal of Information Security and Applications	291	26.45	19.54
Khonji i in. (2013)	IEEE Communications Surveys i Tutorials	266	20.46	16.64
Hong (2012)	Communications of the ACM	264	18.86	12.33
Grier i in. (2010)	ACM Conference on Computer and Communications Security	261	16.31	7.61
Egelman i in. (2008)	CHI Conference Proceedings	259	14.39	17.13

[a)] Cytowania znormalizowane (*normalized citations*) to miara uwzględniająca wiek publikacji i średnią liczbę cytowań w danym roku, obliczana jako liczba cytowań podzielona przez średnią liczbę cytowań dla publikacji z tego samego roku. Wartość powyżej 1 wskazuje na ponadprzeciętny wpływ publikacji.

Źródło: opracowanie własne na podstawie danych z bazy WoS, sporządzone za pomocą narzędzia bibliometrix.

Rysunek 2. Trendy tematyczne w badaniach nad phishingiem, w latach 2006–2024, według słów kluczowych



Legenda: wielkość kół odzwierciedla liczbę publikacji zawierających dane słowo kluczowe w danym roku, a poziome linie pokazują okres występowania tematu w analizowanej literaturze.

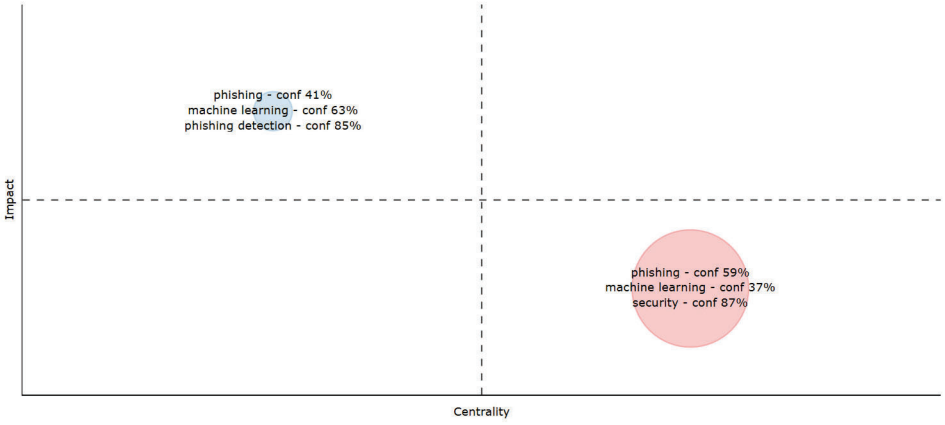
Źródło: opracowanie własne na podstawie danych z bazy WoS, sporządzone za pomocą narzędzia bibliometrix.

Rysunek 2 zawiera zestaw pojęć wykorzystywanych w badaniach nad phishingiem w latach 2006–2024, ilustrując przejście od wczesnych zagadnień technicznych, jak web spoofing i trusted computing (2006–2009), poprzez rozwój metod wykrywania opartych na klasyfikacji bayesowskiej i analizie behawioralnej (2010–2015), aż po zastosowania uczenia maszynowego, sztucznej inteligencji, i technologii blockchain (2020–2024). Najczęściej występującym terminem jest „phishing" (1326 wystąpień), następnie „machine learning" (495 wystąpień) i „security" (436 wystąpień). Rysunek 2 symbolicznie ilustruje transformację paradygmatu badawczego od tradycyjnych metod obrony opartych na regułach i filtrach (spam filtering, anti-phishing) w latach 2013–2016, w kierunku zaawansowanych metod sztucznej inteligencji, przetwarzania języka naturalnego i deep learning w ostatnich latach (2021–2024), co oznacza m.in. rosnące znaczenie automatyzacji i inteligentnych systemów w walce z phishingiem. Szczególnie zauważalny jest wzrost zainteresowania technologiami blockchain i ethereum od 2022 roku, sugerując adaptację nowych podejść do bezpieczeństwa cybernetycznego w kontekście zdecentralizowanych systemów finansowych.

Warto zauważyć, że najbardziej produktywni autorzy (tabela 2) nie pokrywają się z autorami najczęściej cytowanych publikacji (tabela 3). Zjawisko to może wynikać z kilku powodów. Po pierwsze, autorzy najczęściej cytowanych prac często publikowali w pionierskim okresie badań (2006–2015), ustanawiając fundamenty dziedziny, podczas gdy autorzy najbardziej produktywni są aktywni w późniejszych latach, rozwijając istniejące koncepcje. Po drugie, przełomowe publikacje mogą mieć więk-

szy wpływ niż wiele prac o charakterze przyrostowym. Po trzecie, różnica ta może odzwierciedlać specjalizację tematyczną – najbardziej produktywni autorzy mogą koncentrować się na wąskich aspektach technicznych, podczas gdy najczęściej cytowane prace mają charakter interdyscyplinarny lub przeglądowy.

Rysunek 3. Klastry tematyczne dotyczące phishingu



Źródło: opracowanie własne na podstawie danych z bazy WoS, sporządzone za pomocą narzędzia bibliometrix.

Rysunek 3 zawiera klastry tematyczne (według Keywords Plus) utworzone na podstawie analizy pozycji literatury dotyczącej phishingu oraz ich sprzężenia przez wspólne cytowania. W ten sposób powstały dwa klastry badawcze o różnych poziomach centralności i wpływu. Klaster 1 (różowy), utworzony na podstawie 137 dokumentów, koncentruje się wokół zagadnień „security", „attacks" i „classification" z poziomami pewności odpowiednio: 79,2%, 62,5% i 59,1%, osiągając centralność 0,401 i wpływ lokalny 7,542. Parametry te wskazują na jego fundamentalną rolę w badaniach nad bezpieczeństwem i klasyfikacją ataków phishingowych. Klaster 2 (niebieski), utworzony na podstawie 113 dokumentów, skupia badania wokół „features", „model" i „websites" z wyższymi poziomami pewności (88,9%, 57,1%, 86,7%) oraz nieznacznie wyższą centralnością (0,399), a także większym wpływem lokalnym (8,411). Wskazuje to koncentrację na modelowaniu i analizie cech technicznych stron internetowych. Uzyskany podział badanych dokumentów na dwa klastry oznacza dychotomię w badaniach nad phishingiem. A mianowicie podejście skupione na analizie zagrożeń bezpieczeństwa oraz podejście skupione na technicznych metodach wykrywania opartych na cechach i modelowaniu. Przy czym drugi klaster cechuje silniejszy wpływ na rozwój badań w tym obszarze, pomimo mniejszej liczby publikacji. Z dużym prawdopodobieństwem wiąże się to z wyższym poziomem innowacyjności i cytowań w badaniach nad algorytmami wykrywania phishingu.

3. Charakterystyka najczęściej cytowanych publikacji dotyczących phishingu w ekonomii i finansach

Phishing jako zjawisko o naturze cyberprzestępczej ma istotne znaczenie dla bezpieczeństwa finansowego, a nawet stabilności sektora bankowego. Tezę tę uzasadnia przede wszystkim szacowana wysokość strat opiewająca na miliardy dolarów rocznie, a także podrywanie zaufania konsumentów do usług finansowych i obrotu w elektronicznych kanałach dystrybucji. W odróżnieniu od publikacji w tabeli 3 poniższy przegląd obejmuje 10 najczęściej cytowanych publikacji z bazy WoS tylko z kategorii „Economy & Business Finance". co umożliwia pogłębioną analizę konsekwencji ekonomicznych i finansowych phishingu dla sektora bankowego.

Herley i Florêncio (2010) w pracy *Nobody Sells Gold for the Price of Silver: Dishonesty, Uncertainty and the Underground Economy* przeprowadzili analizę nielegalnej gospodarki cybernetycznej, szczególnie koncentrując się na rynkach IRC[1] oferujących skradzione tożsamości, zestawy phishingowe, botnety[2] i usługi związane z cyberprzestępczością. Autorzy udowodnili istnienie wyrafinowanych 'podziemnych' rynków charakteryzujących się wysokim poziomem specjalizacji i dojrzałości, z kompleksowym podziałem pracy i ofertą usług, co zrewolucjonizowało spojrzenie na ekonomiczne aspekty cyberprzestępczości. Praca ta była cytowana 62 razy i miała kapitalne znaczenie dla zrozumienia mechanizmów ekonomicznych napędzających ataki phishingowe. Hornuf i in. (2022) w badaniu „Initial coin offerings, information disclosure, and fraud" opublikowanym w „Small Business Economics" przeprowadzili kompleksową analizę oszustw w Initial Coin Offerings (ICO), dokumentując różne rodzaje oszustw i wykazując, że oszukańcze ICO są średnio znacznie większe niż przeciętne dla innych oszustw. Autorzy odkryli paradoks, zgodnie z którym emitenci ujawniający swój kod na GitHub[3] są bardziej narażeni na ataki phishingowe i hakerskie, co wskazuje na ryzyko transparencji. Ta publikacja, cytowana 54 razy, wniosła kluczowy wkład w zrozumienie związku między ujawnianiem informacji a podatnością na cyberprzestępstwa w sektorze finansowym.

Shkarlet i in. (2018) w pracy *Determinants of the Financial Services Market Functioning in the Era of the Informational Economy Development* opublikowanej w „Baltic

[1] Rynek IRC nie istnieje jako rynek finansowy czy handlowy w klasycznym rozumieniu. IRC to przede wszystkim technologia komunikacyjna (ang. Internet Relay Chat), czyli sieć kanałów rozmów online. W Polsce funkcjonują różne sieci IRC, np. PIRC.PL, które można nazwać „rynkiem" w sensie społecznościowym jako miejsce i sposób wymiany informacji, kontaktów i usług. Działa w architekturze klient–serwer: użytkownik łączy się z serwerem IRC za pomocą programu-klienta, a rozmowy odbywają się na kanałach tematycznych. Kanały mogą być publiczne (otwarte dla wszystkich) lub prywatne (tylko dla zaproszonych).

[2] Botnety to sieci urządzeń (komputerów, smartfonów, serwerów czy sprzętu IoT) zainfekowanych złośliwym oprogramowaniem, które są zdalnie kontrolowane przez cyberprzestępców. Każde urządzenie w takiej sieci działa jak „bot" i wykonuje polecenia operatora bez wiedzy właściciela.

[3] GitHub to największa na świecie platforma do współpracy nad kodem, oparta na systemie kontroli wersji Git. Umożliwia programistom przechowywanie projektów, śledzenie zmian, współpracę zespołową i publikowanie oprogramowania w modelu *open source* lub prywatnym.

Journal of Economic Studies" określili determinanty funkcjonowania rynku usług finansowych w erze rozwoju gospodarki informacyjnej. Autorzy wykazali obiektywne powiązania między systemami finansowymi a gospodarką narodową, podkreślając transformacyjny wpływ technologii informacyjnych na funkcjonowanie instytucji finansowych. Ta publikacja, cytowana 17 razy, dostarczyła teoretycznych ram dla zrozumienia wpływu digitalizacji na bezpieczeństwo sektora finansowego.

Bayl-Smith i in. (2020) w badaniu „Cue Utilization, Phishing Feature and Phishing Email Detection", zaprezentowanym na 24th International Conference on Financial Cryptography and Data Security opracowali koncepcję wskazówek jako unikalnego predyktora wykrywania cech phishingu. Badanie przeprowadzone na 127 studentach psychologii wykazało znaczenie procesów kognitywnych w identyfikacji e-maili phishingowych. Ta praca, cytowana 12 razy, przyczyniła się do lepszego zrozumienia psychologicznych mechanizmów podatności na phishing w kontekście finansowym.

O'Leary (2019) w artykule *What Phishing E-mails Reveal: An Exploratory Analysis of Phishing Attempts Using Text Analysis* opublikowanym w „Journal of Information Systems" przeprowadził analizę tekstową e-maili phishingowych skierowanych przeciwko księgowym i firmom audytorskim. Porównując bazę danych wiadomości phishingowych z e-mailami Enron, autor wykazał statystycznie istotne różnice w wielu kategoriach zmiennych tekstowych. Ta publikacja, cytowana 11 razy, wygenerowała model phishingu jako «władzy» oparty na zmiennych: przyjaciel, osiągnięcie, pieniądze i praca, co stało się podstawą do późniejszych badań nad analizą tekstową w kontekście finansowym.

Bakarich i Baranek (2020) w studium przypadku „Something Phish-y is Going On Here: A Teaching Case on Business Email Compromise" opublikowanym w „Current Issues in Auditing" przeanalizowali przypadek amerykańskiej spółki publicznej, która padła ofiarą oszustwa nazwanego Business Email Compromise (BEC), w wyniku którego pracownik nieumyślnie przelał miliony dolarów na oszukańcze konta. Ta publikacja, cytowana 8 razy, dostarczyła cennych wniosków edukacyjnych dla sektora audytorskiego i finansowego dotyczących rosnącej prevalencji i skali tego typu oszustw korporacyjnych.

Das i in. (2020) w pracy *User-Centered Risk Communication for Safer Browsing* zaprezentowanej na 24th International Conference on Financial Cryptography and Data Security opracowali narzędzie zarządzania ryzykiem łączące spersonalizowane blokowanie, filtrowanie i alerty w pojedynczy system holistyczny. Autorzy wykorzystali proste metaforyczne ilustracje funkcjonujące zarówno jako komunikacja ryzyka, jak i kontrole ustawień przeglądarki. Ta publikacja, cytowana 7 razy, wniosła istotny wkład w rozwój user-centered podejścia do bezpieczeństwa finansowego online.

Taylor-Jackson i in. (2020) w opracowaniu *Incorporating Psychology into Cyber Security Education: A Pedagogical Approach* zaprezentowanym na 24th International Conference on Financial Cryptography and Data Security podkreślili rolę czynnika ludzkiego w cyberbezpieczeństwie. Autorzy wykazali, że wiele incydentów cyberbezpieczeństwa polega na skłonieniu celowo wybranych osób do wykonania określonych zachowań lub działań, jak np. otwarcie linku w e-mailu phishingowym. Ta publikacja,

cytowana 7 razy, przyczyniła się do rozwoju pedagogicznych podejść uwzględniających psychologię w edukacji cyberbezpieczeństwa finansowego.

Basu (2018) w pracy *Markets and Manipulation: Time for a Paradigm Shift?* opublikowanej w „Journal of Economic Literature" przedstawił przegląd rosnącego znaczenie w ekonomii ludzkich słabości emocjonalnych, przywiązania do norm społecznych oraz systematycznych irracjonalności, wpływających na podejmowanie decyzji rynkowych. Autor podkreślił, że istoty ludzkie są podatne na manipulację ze strony pozbawionych skrupułów agentów wykorzystujących marketing swoich usług lub towarów. Ta publikacja, cytowana 6 razy, dostarczyła ram poznawczych dla zrozumienia psychologicznych podstaw podatności na oszustwa finansowe.

Olifer i in. (2017) w badaniu „Controls-Based Approach for Evaluation of Information Security Standards Implementation Costs" opublikowanym w „Technological and Economic Development of Economy" przeprowadzili analizę kosztów implementacji standardów bezpieczeństwa informacji. Autorzy wykazali, że według analizy PricewaterhouseCoopers średni koszt pojedynczego naruszenia bezpieczeństwa informacji i ochrony danych wzrósł dwukrotnie w 2015 roku, a liczba organizacji zgłaszających poważne naruszenia wzrosła z 9% w 2015 roku do 17% w 2016 roku. Ta publikacja, cytowana 6 razy, dostarczyła fundamentalnych danych ekonomicznych dotyczących kosztów cyberprzestępczości dla sektora finansowego.

Podsumowanie

Przeprowadzona analiza bibliometryczna literatury naukowej dotyczącej phishingu, ze szczególnym uwzględnieniem sektora finansowego, charakteryzuje stan badań w nad tym zjawiskiem, wskazuje główne tendencje i kierunki rozwoju. Dynamika zainteresowania badawczego phishingiem, odzwierciedlona roczną stopą wzrostu publikacji wynoszącą 16,35%, potwierdza rosnące zagrożenie z jego strony dla bezpieczeństwa cybernetycznego instytucji finansowych oraz pilną potrzebę systematycznych badań naukowych (Donthu i in. 2021).

Ewolucja paradygmatów badawczych phishingu w latach 2003–2024 wskazuje na przejście od tradycyjnych podejść opartych na analizie technicznej i regułach w kierunku zaawansowanych metod wykorzystujących sztuczną inteligencję, uczenie maszynowe i przetwarzanie języka naturalnego. Od 2022 roku zauważalne jest intensywne zainteresowanie technologiami blockchain i ethereum, co sygnalizuje eksplorację nowych mechanizmów bezpieczeństwa w kontekście zdecentralizowanych systemów finansowych (Sahingoz i in. 2019; Das i in. 2020). Zamieszczanie licznych publikacji z tego obszaru w prestiżowych czasopismach, jak IEEE Access (135 publikacji) oraz Computers & Security (104 publikacje) wskazuje na istnienie uznanych platform publikacyjnych w dziedzinie badań nad phishingiem. Natomiast dominacja publikacji w formule open access odzwierciedla trend w upowszechnianiu wyników badań nad cyberbezpieczeństwem. Jednocześnie, globalny charakter współpracy badawczej, reprezentowany przez wiodące instytucje z Ameryki Pół-

nocnej, Azji i Bliskiego Wschodu podkreśla uniwersalny charakter zagrożeń phishingowych oraz potrzebę międzynarodowej koordynacji działań badawczych.

Analiza klastrów tematycznych ujawnia wyraźną dychotomię między badaniami skupionymi na analizie zagrożeń bezpieczeństwa a metodami technicznymi wykrywania opartymi na cechach i modelowaniu, przy czym drugi klaster wykazuje silniejszy wpływ na rozwój dziedziny, co sugeruje większą innowacyjność w obszarze algorytmów wykrywania phishingu.

Przegląd najczęściej cytowanych publikacji z zakresu phishingu z perspektywy ekonomiczno-finansowej wskazuje na fundamentalne znaczenie prac Herley i Florêncio (2010) dotyczących ekonomiki podziemnej gospodarki cybernetycznej oraz rosnące znaczenie badań nad ICO i cryptocurrency w kontekście oszustw finansowych (Hornuf i in. 2022). Identyfikacja luk badawczych wskazuje na potrzebę intensyfikacji badań w kilku kluczowych obszarach. Po pierwsze, niezbędne są interdyscyplinarne badania łączące aspekty techniczne z behawioralnymi, uwzględniające specyficzne charakterystyki użytkowników usług finansowych oraz kulturowe determinanty podatności na phishing. Po drugie, wymaga pogłębienia analiza długoterminowych skutków ekonomicznych ataków phishingowych dla stabilności sektora bankowego oraz efektywności różnych strategii inwestycyjnych w cyberbezpieczeństwo. Po trzecie, niezbędne są badania nad etyką zastosowania sztucznej inteligencji w wykrywaniu phishingu, szczególnie w kontekście ochrony prywatności klientów instytucji finansowych.

Przyszłe kierunki badań powinny koncentrować się na rozwoju personalizowanych systemów wykrywania phishingu wykorzystujących zaawansowane algorytmy uczenia maszynowego dostosowane do specyficznych profili ryzyka użytkowników usług bankowych. Szczególnie perspektywiczne wydają się badania nad zastosowaniem technologii blockchain w tworzeniu zdecentralizowanych systemów weryfikacji tożsamości oraz wykorzystaniem przetwarzania języka naturalnego do analizy semantycznej komunikacji phishingowej w czasie rzeczywistym. Implikacje praktyczne przeprowadzonej analizy wskazują na konieczność zintegrowanego podejścia do cyberbezpieczeństwa w instytucjach finansowych, łączącego zaawansowane rozwiązania technologiczne z systematyczną edukacją użytkowników oraz regularnymi ocenami podatności organizacyjnej. Rekomendacje dla praktyków obejmują inwestycje w wielowarstwowe systemy obrony, rozwój kultur bezpieczeństwa organizacyjnego oraz tworzenie mechanizmów współpracy międzynarodowej w zakresie wymiany informacji o zagrożeniach.

Niniejsza analiza bibliometryczna potwierdza, że badania nad phishingiem w sektorze finansowym znajdują się w fazie intensywnego rozwoju, charakteryzującej się rosnącym zaawansowaniem metodologicznym oraz integracją różnych dyscyplin naukowych. Przyszłość tej dziedziny będzie prawdopodobnie kształtowana przez postępy w sztucznej inteligencji, rozwoju technologii blockchain oraz rosnące znaczenie czynników behawioralnych w projektowaniu systemów cyberbezpieczeństwa, co wymaga kontynuacji systematycznych badań naukowych oraz ścisłej współpracy między środowiskiem akademickim a praktykami sektora finansowego.

Bibliografia

Abdajabar A., Idbeaa, T. (2024). *Cybercrime's Threat to Financial Institutions During COVID-19*. AlQalam Journal of Medical and Applied Sciences, 46–52.

Anderson R., Moore T. (2006). *The economics of information security*. Science, 314(5799), 610–613.

Aria M., Cuccurullo C. (2017). *Bibliometrix: An R-tool for comprehensive science mapping analysis*. „Journal of Informetrics", 11(4), 959–975.

Bakarich K.M., Baranek D. (2020). *Something phish-y is going on here: A teaching case on business email compromise*. „Current Issues in Auditing", 14(1), A1–A9. https://doi.org/10.2308/ciia-52706

Basu K. (2018). *Markets and manipulation: Time for a paradigm shift?* „Journal of Economic Literature", 56(1), 185–205. https://doi.org/10.1257/jel.20161410

Bayl-Smith P., Sturman D., Wiggins M. (2020). *Cue utilization, phishing feature and phishing email detection*, [w:] *Financial Cryptography and Data Security*, FC 2020 (s. 56–70). Springer. https://doi.org/10.1007/978-3-030-54455-3_5

Bhatt P., Obaidat M.S., Dangwal G., Das A.K., Wazid M., Sadoun B. (2024). *Machine learning-based security mechanism for detecting phishing attacks*, [w:] *2024 International Conference on Communications, Computing, Cybersecurity, and Informatics (CCCI)* (s. 1–6). IEEE. https://doi.org/10.1109/CCCI61916.2024.10736460

Das S., Abbott J., Gopavaram S., Blythe J., Camp L. J. (2020). *User-centered risk communication for safer browsing*, [w:] *International conference on financial cryptography and data security* (s. 18–35). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-030-54455-3_2

Do N.Q., Selamat A., Krejcar O., Herrera-Viedma E., Fujita H. (2022). *Deep learning for phishing detection: Taxonomy, current challenges and future directions*. Ieee Access, 10, 36429–36463. https://doi.org/10.1109/ACCESS.2022.3151903

Donthu N., Kumar S., Mukherjee D., Pandey N., Lim W.M. (2021). *How to conduct a bibliometric analysis: An overview and guidelines*. „Journal of business research", 133, 285–296.

Egelman S., Cranor L.F., Hong J. (2008). *You've been warned: An empirical study of the effectiveness of web browser phishing warnings*. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, 1065–1074.

Grier C., Ballard L., Caballero J., Chachra N., Dietrich C.J., Levchenko K., …, Voelker G.M. (2010). *Manufacturing compromise: The emergence of exploit-as-a-service*. Proceedings of the 17th ACM Conference on Computer and Communications Security, 821–832. https://doi.org/10.1145/1866307.1866311

Herley C., Florêncio D. (2010). *Nobody sells gold for the price of silver: Dishonesty, uncertainty and the underground economy*, [w:] *Economics of Information Security and Privacy* (s. 33–53). Springer. https://doi.org/10.1007/978-1-4419-6967-5_3

Hong J. (2012). *The state of phishing attacks*. Communications of the ACM, 55(1), 74–81. https://doi.org/10.1145/2063176.2063197

Hornuf L., Kück T., Schwienbacher A. (2022). *Initial coin offerings, information disclosure, and fraud*. „Small Business Economics", 58(4), 1741–1759. https://doi.org/10.1007/s11187-021-00471-y

Jagatic T.N., Johnson N.A., Jakobsson M., Menczer F. (2007). *Social phishing*. „Communications of the ACM", 50(10), 94–100. https://doi.org/10.1145/1290958.1290968

Khonji M., Iraqi Y., Jones A. (2013). *Phishing detection: A literature survey*. IEEE Communications Surveys i Tutorials, 15(4), 2091–2121. https://doi.org/10.1109/SURV.2013.032213.00009

Król P. (2024). *Phishing jako zagrożenie dla bezpieczeństwa bankowości cyfrowej*. „Bezpieczny Bank", 94(1), 25–42. https://doi.org/10.26354/bb.2.1.94.2024

Krombholz K., Hobel H., Huber M., Weippl E. (2015). *Advanced social engineering attacks*. „Journal of Information Security and Applications", 22, 113–122. https://doi.org/10.1016/j.jisa.2014.09.005

Mutlutürk M., Metin B. (2023). *Mapping The Phishing Attacks Research Landscape: A Bibliometric Analysis And Taxonomy*. „J. Theor. Appl. Inf. Technol", 101, 6758–6780.

Mutlutürk M., Wynn M., Metin B. (2024). *Phishing and the Human Factor: Insights from a Bibliometric Analysis*. „Information", 15(10), 643. https://doi.org/10.3390/info15100643

Mwavali A. (2024). *Combating phishing in Kenya: A supervised learning model for enhanced email security in Kenyan financial institutions*. „International Journal of Technology and Systems", 9(4), 23–36.

Nwafor K.C., Ikudabo A.O., Onyeje C.C., Ihenacho D.O.T. (2024). *Mitigating cybersecurity risks in financial institutions: The role of AI and data analytics*. „International Journal of Science and Research Archive", 13(01), 2895–2910.

O'Leary D.E. (2019). *What phishing e-mails reveal: An exploratory analysis of phishing attempts using text analysis*. „Journal of Information Systems", 33(3), 285–307. https://doi.org/10.2308/isys-52481

Olifer D., Goranin N., Kaceniauskas A., Cenys A. (2017). *Controls-based approach for evaluation of information security standards implementation costs*. „Technological and Economic Development of Economy", 23(1), 196–219. https://doi.org/10.3846/20294913.2017.1280558

Olowu O., Adeleye A.O., Omokanye A.O., Ajayi A.M., Adepoju A.O., Omole O.M., Chianumba E.C. (2024). *AI-driven fraud detection in banking: A systematic review of data science approaches to enhancing cybersecurity*. „Advanced Research and Review", 21(2), 227–237.

Perwej Y., Abbas S.Q., Dixit J.P., Akhtar N., Jaiswal A.K. (2021). *A systematic literature review on the cyber security*. „International Journal of scientific research and management{, 9(12), 669–710.

Sahingoz O.K., Buber E., Demir O., Diri B. (2019). *Machine learning based phishing detection from URLs*. „Expert Systems with Applications{, 117, 345–357. https://doi.org/10.1016/j.eswa.2018.09.029

Sheng S., Holbrook M., Kumaraguru P., Cranor L.F., Downs J. (2010). *Who falls for phish? A demographic analysis of phishing susceptibility and effectiveness of interventions*. „Proceedings of the SIGCHI Conference on Human Factors in Computing Systems", 373–382.

Shkarlet S., Dubyna M., Zhuk O. (2018). *Determinants of the financial services market functioning in the era of the informational economy development*. „Baltic Journal of Economic Studies", 4(3), 349–357. https://doi.org/10.30525/2256-0742/2018-4-3-349-357

Taylor-Jackson J., McAlaney J., Ashenden D., Dale J. (2020). *Incorporating psychology into cyber security education: A pedagogical approach*, [w:] *Financial Cryptography and Data Security*, FC 2020 (s. 207–217). Springer. https://doi.org/10.1007/978-3-030-54455-3_15

Villanueva J., Sebastian J., Dextre J. (2024, July). *Web Portal Validation Model by Digital Signature and ISO 27002 to Reduce Private Credentials Theft for Phishing Attacks to Financial Sector Customers*, [w:] *2024 International Conference on Electrical, Computer and Energy Technologies (ICECET)* (s. 1–5). IEEE.

Xiang G., Hong J., Rose C.P., Cranor L. (2011). *CANTINA+: A feature-rich machine learning framework for detecting phishing web sites*. „ACM Transactions on Information and System Security", 14(2), 1–28. https://doi.org/10.1145/2019599.2019606

Yuspin W., Putri A.O., Fauzie A., Pitaksantayothin J. (2024). *Digital Banking Security: Internet Phishing Attacks, Analysis and Prevention of Fraudulent Activities*. „International Journal of Safety & Security Engineering", 14(6).

Zhuo S., Biddle R., Koh Y.S., Lottridge D., Russello G. (2023). *SoK: Human-centered phishing susceptibility*. „ACM Transactions on Privacy and Security", 26(3), 1–27.