Julia Dymek

e-mail: 181441@student.ue.wroc.pl
ORCID: 0009-0008-0600-8552

Uniwersytet Ekonomiczny we Wrocławiu

Badanie poziomu realizacji założeń cyberbezpieczeństwa firm i instytucji Unii Europejskiej

DOI: 10.15611/2024.76.5.08
JE: C38, K24

Cytuj jako: Dymek, J. (2024). Badanie poziomu realizacji założeń cyberbezpieczeństwa firm i instytucji Unii Europejskie. W: A. Stanimir (red.), *Współczesne problemy społeczno-ekonomiczne w ujęciu analitycznym* (s. 117-131). Wydawnictwo Uniwersytetu Ekonomicznego we Wrocławiu.

Streszczenie: Cyberbezpieczeństwo jest bardzo ważnym tematem, o którym coraz częściej się mówi oraz słyszy. Zyskało ono na znaczeniu wraz z rozwojem technologicznym. Celem artykułu jest zbadanie sytuacji w obszarze cyberbezpieczeństwa w małych i średnich przedsiębiorstwach krajów Unii Europejskiej oraz omówienie form zabezpieczenia firm przed cyberzagrożeniami. W tym celu przeprowadzono dwutorową analizę za pomocą klasyfikacji hierarchicznej oraz porządkowania liniowego ważoną metodą sum standaryzowanych. Zaczerpnięte dane pochodzą z badania przeprowadzonego przez Ipsos European Public Affairs. Analiza i wynikające z niej wnioski potwierdziły hipotezy o tym, że bogatsze i bardziej rozwinięte kraje znajdą się w jednym skupieniu oraz państwa Europy Zachodniej i Północnej będą plasowały się wysoko w utworzonych rankingach.

Słowa kluczowe: cyberbezpieczeństwo, cyberprzestępstwo, łańcuch bloków, klasyfikacja hierarchiczna, porządkowanie liniowe

1. Wstęp

Rozwój technologiczny oraz rewolucja cyfrowa są nieodłącznymi elementami współczesnego świata. Wskutek pandemii COVID-19 pojawiło się więcej możliwości załatwienia spraw służbowych oraz prywatnych przez Internet. Jednakże wraz z postępem technologicznym zaczęło zyskiwać na znaczeniu cyberbezpieczeństwo. Zjawisko z nim powiązane to cyberprzestępstwo. Szafranek (2021) na podstawie przeprowadzonych badań i opublikowanych przez CERT Polska raportów stwierdził, iż w latach 2010-2020 można zauważyć wzrost liczby zgłaszanych cyberprzestępstw. Najczęstsze rodzaje przeprowadzanych ataków to między innymi: włamania do sieci wewnętrznej Intranet, phishing, ataki na serwery, kradzieże tożsamości, spam czy ataki szkodliwego oprogramowania (Maciejowski, 2004, za: Szafranek 2021).

W związku z tym w niniejszym artykule postanowiono zgłębić temat związany z cyberbezpieczeństwem. Za cele obrano zbadanie w głównej mierze tego, jak wygląda sytuacja w małych i średnich przedsiębiorstwach krajów Unii Europejskiej w tym obszarze oraz w jaki sposób można zabezpieczyć firmę przed cyberzagrożeniami i wynikającymi z nich skutkami.

Przeprowadzono analizy z wykorzystaniem klasyfikacji hierarchicznej oraz porządkowania liniowego. Wskazane metody wybrano, by określić, które kraje Unii Europejskiej są podobne do siebie pod względem badanych zmiennych odzwierciedlających sytuację panującą w małych i średnich przedsiębiorstwach w obszarze cyberbezpieczeństwa. Przystępując do badania, postawiono następujące hipotezy badawcze:

- *H*1: bogatsze i bardziej rozwinięte kraje stanowią spójną grupę pod względem cyberbezpieczeństwa,
- *H*2: kraje Europy Zachodniej i Północnej plasują się wysoko w rankingach ze względu na analizowane zmienne.

Do badania wzięto pod uwagę zmienne dotyczące:

- poziomu obaw pracowników wobec cyberataków,
- podejmowanych działań, jak na przykład przeprowadzenie szkolenia wśród zatrudnionych,
- tego, w jakim stopniu są oni zorientowani w kwestii niebezpieczeństw wynikających z cyberprzestępczości.

2. Cyberbezpieczeństwo – definicja i inne jego aspekty

Dział cyberbezpieczeństwa Departamentu Bezpieczeństwa Wewnętrznego w Stanach Zjednoczonych opisuje cyberbezpieczeństwo jako pewien proces, zdolność, stan, który przyczynia się do tego, iż wszelkie informacje i systemy komunikacyjne oraz wszystkie dane w nich zawarte są zabezpieczone w razie zniszczenia, modyfikacji czy nieprawnego wykorzystania przez osoby trzecie (Bay, 2016).

W cyberbezpieczeństwie dużą rolę odgrywa sformułowane w 1965 roku przez Gordona Moore'a, współzałożyciela firmy Intel, prawo Moore'a (Cunningham, 2021). Dzięki obserwacjom stale rozwijających się trendów zdołał on oszacować tempo rozwoju nowoczesnej cyfrowej rewolucji. Należy również zaznaczyć, iż firma Intel (b.d.) stwierdziła, że prawo to uzyskało miano złotej zasady przemysłu elektronicznego. Pierwotnie odnosiło się ono do tempa podwajania się liczby tranzystorów w układach scalonych. Jednakże wykazuje też, że zapotrzebowanie na wzrost mocy obliczeniowej zmienia się z biegiem czasu zgodnie z trendem wykładniczym (Cunningham, 2021). Moc obliczeniowa dotyczy wydajności danego komputera. Zgodnie z fizycznym wzorem na moc można dowiedzieć się, jaką ilość pracy wykonał komputer w określonym czasie (Ghosh, 2012). Cunningham (2021) stwierdził, iż w związku z postępującym rozwojem technologii występuje coraz więcej zagrożeń w cyberprzestrzeni.

Cyberprzestępcy atakują przedsiębiorstwa zarówno małe, średnie, jak i duże. Warto przytoczyć incydent dotyczący firmy, która zajmuje się marketingiem oraz tworzeniem marki i zatrudnia 25 osób. Jeden z pracowników padł ofiarą phishingu. Wskutek tego cyberprzestępcy przejęli jego konto mailowe i wysłali z niego wiadomości do klientów. Jedne z nich miały na celu dalsze przeprowadzanie ataków phishingowych, a pozostałe dostarczały fałszywy komunikat o tym, iż firma zmieniła dane dotyczące konta bankowego, na które należy przelewać należności. Jednakże podane w wiadomości konto należało do przestępców. Jedno z przedsiębiorstw, które korzystało z usług opisywanej organizacji, wykryło nieprawidłowość i zgłosiło, że otrzymane e-maile są nieprawdziwe. W ostateczności klient zerwał umowę i wszystkie nadchodzące przelewy pieniężne opiewające nawet na 300 tysięcy euro zostały unieważnione (European Union Agency for Cybersecurity, 2021).

Celem cyberprzestępców stały się małe firmy, ponieważ zatrudniają niewielką liczbę pracowników. Dodatkowo osoby pełniące ważne funkcje w firmie oraz administratorzy są bardzo często przepracowani, co wpływa negatywnie na ich koncentrację i może skutkować brakiem zachowania ostrożności w podejmowaniu decyzji. Ponadto z racji tego, iż przedsiębiorstwa te korzystają ze starszych rozwiązań technologicznych, niż są aktualnie dostępne, firmowe sieci nie są w odpowiedni sposób skonfigurowane i zabezpieczone (Cunningham, 2021). Ważny jest też fakt, iż małe i średnie firmy niejednokrotnie nawiązują współpracę z większymi przedsiębiorstwami przykładowo stają się one ich dostawcami, partnerami czy też podwykonawcami podczas realizacji konkretnego procesu (Cunningham, 2021; Williamson, 2014, za Choi i Allison, 2017). W związku z tym cyberprzestępcy, włamując się na konta mniejszych przedsiębiorstw, mogą również uzyskać nieautoryzowany dostęp do poufnych informacji czy danych dotyczących większych firm.

Warto również wspomnieć o kosztach związanych z cyberbezpieczeństwem ponoszonych przez przedsiębiorstwo. Można wyróżnić koszty pośrednie oraz bezpośrednie. Koszty pośrednie to takie, których wartość można przewidzieć i dotyczą one zapobiegania atakom ze strony hakerów. Zaliczane są do nich między innymi: szkolenia pracowników z zakresu cyberbezpieczeństwa, ubezpieczenie od ryzyka cybernetycznego, doradztwo specjalistyczne, wynagrodzenia pracowników dbających o cyberbezpieczeństwo, zakup licencji na programy antywirusowe oraz koszty związane z bezpieczeństwem danych. Koszty bezpośrednie wiążą się z naprawą szkód wywołanych cyberprzestępczością. Do tej kategorii kosztów należą: koszty związane z ochroną konsumenta w momencie wycieku danych osobowych, opłata za usługi prawne, koszt odzyskania utraconych danych, naruszenie wizerunku, utrata środków pieniężnych w wyniku włamania na konto bankowe firmy oraz utrata własności intelektualnej (Antczak, 2020).

Organizacje są zmuszone szukać nowych rozwiązań, które pozwolą zabezpieczyć firmę przed atakami cyberprzestępców (Szafranek, 2021). Niezmiernie istotną kwestią jest technologia *blockchain*. Jest to łańcuch bloków, w których zapisywane są różnego rodzaju dane, między innymi dotyczące transakcji handlowych (Bambara

i Allen, 2018). Dane są niezmienne, nieodwracalne i zdecentralizowane, czyli rozproszone nawet po całym świecie (Mathew, 2019). Nie są one gromadzone na jednym komputerze, tylko na wielu urządzeniach. Każdy blok, oprócz tego, że zawiera dane, charakterystyczny dla niego hash, to ma również hash bloku poprzedniego. (Bambara i Allen, 2018; Mathew, 2019;). To oznacza, że dysponuje również informacjami o bloku poprzednim. Hash można określić jako pewien ciąg znaków, dzięki któremu można zaszyfrować ważne komunikaty. Jest to zaleta technologii *blockchain*, ponieważ w przypadku, gdy osoba trzecia będzie chciała zmodyfikować dane znajdujące się w danym bloku, to spowoduje, iż zostanie zaburzona integralność łańcucha (Mathew, 2019). Warto także scharakteryzować dwa systemy, które mogą pomóc w walce z cyberprzestępczością. Pierwszy z nich to system wykrywania włamań *Intrusion Detection System* (IDS). Jest on zaliczany do pasywnych systemów bezpieczeństwa, ponieważ nie podejmuje on żadnych czynności celem ochrony przed nieprawnym dostaniem się osób trzecich czy złośliwych oprogramowań do systemów (Choi i Allison, 2017). Stosuje się go do obserwowania aktywności w sieci. Drugi równie ważny system to system zapobiegania włamaniom – *Intrusion Prevention System* (IPS). Jego zadaniem jest zidentyfikowanie zagrożeń w sieci oraz podejmowanie kroków, aby ochronić sieć (Chakraborty, 2013).

3. Metodyka badań

3.1. Charakterystyka wykorzystanych zmiennych

Zbiór danych, z którego skorzystano w przeprowadzonej analizie, powstał na podstawie badania, które zostało zlecone przez Komisję Europejską i Dyrekcję Generalną do spraw Polityki Regionalnej i Miejskiej. Wskazane badanie było koordynowane przez Dyrekcję Generalną do spraw Komunikacji. Przeprowadzone zostało w formie wywiadów telefonicznych między 26 listopada 2021 r. a 17 grudnia 2021 r. przez Ipsos European Public Affairs. Zbadano małe i średnie przedsiębiorstwa w krajach Unii Europejskiej, w których liczba pracowników jest mniejsza niż 250. Firmy te działają w następujących obszarach: produkcyjnym, usługowym, sprzedaży detalicznej oraz przemysłowym. Rozmowy telefoniczne prowadzone były z najważniejszymi osobami w przedsiębiorstwie, między innymi z: głównym menadżerem, dyrektorem finansowym, prezesem zarządu czy menadżerem sprzedaży i marketingu (European Commission, 2022).

Do przeprowadzenia analizy wzięto pod uwagę następujące zmienne:

- X_1 – procent firm, w których pracownicy są w ogóle niepoinformowani o zagrożeniach związanych z cyberprzestępczością,
- X_2 – procent firm, w których najważniejsza osoba, pełniąca funkcje decyzyjne, jest bardzo zaniepokojona wirusami, *spyware* lub *malware* podczas korzystania z Internetu, wykonując działania związane z biznesem, takie jak sprzedaż towarów lub usługi bankowości internetowej,

- X_3 – procent firm, w których najważniejsza osoba, pełniąca funkcje decyzyjne, jest bardzo zaniepokojona phishingiem, przejęciem konta lub podszywaniem się podczas korzystania z Internetu, wykonując działania związane z biznesem, takie jak sprzedaż towarów lub usługi bankowości internetowej,
- X_4 – procent firm, w których najważniejsza osoba, pełniąca funkcje decyzyjne, jest bardzo zaniepokojona ransomware podczas korzystania z Internetu, wykonując działania związane z biznesem, takie jak sprzedaż towarów lub usługi bankowości internetowej,
- X_5 – procent firm, w których w ciągu ostatnich 12 miesięcy firma nie przeprowadziła szkolenia pracowników lub nie podniosła świadomości na temat zagrożeń związanych z cyberprzestępczością,
- X_6 – procent firm, w których najważniejsza osoba, pełniąca funkcje decyzyjne, jest bardzo zaniepokojona zhakowaniem internetowego konta bankowego firmy podczas korzystania z Internetu, wykonując działania związane z biznesem, takie jak sprzedaż towarów lub usługi bankowości internetowej,
- X_7 – procent firm, w których pracownicy są bardzo dobrze poinformowani o zagrożeniach związanych z cyberprzestępczością,
- X_8 – procent firm, w których najważniejsza osoba, pełniąca funkcje decyzyjne, w ogóle nie jest zaniepokojona wirusami, *spyware* lub *malware* podczas korzystania z Internetu, wykonując działania związane z biznesem, takie jak sprzedaż towarów lub usługi bankowości internetowej,
- X_9 – procent firm, w których najważniejsza osoba, pełniąca funkcje decyzyjne, w ogóle nie jest zaniepokojona phishingiem, przejęciem konta lub podszywaniem się podczas korzystania z Internetu, wykonując działania związane z biznesem, takie jak sprzedaż towarów lub usługi bankowości internetowej,
- X_{10} – procent firm, w których najważniejsza osoba, pełniąca funkcje decyzyjne, w ogóle nie jest zaniepokojona *ransomware* podczas korzystania z Internetu, wykonując działania związane z biznesem, takie jak sprzedaż towarów lub usługi bankowości internetowej,
- X_{11} – procent firm, w których w ciągu ostatnich 12 miesięcy firma przeprowadziła szkolenie pracowników lub podniosła świadomość na temat zagrożeń związanych z cyberprzestępczością,
- X_{12} – procent firm, w których najważniejsza osoba, pełniąca funkcje decyzyjne, w ogóle nie jest zaniepokojona zhakowaniem internetowego konta bankowego firmy podczas korzystania z Internetu, wykonując działania związane z biznesem, takie jak sprzedaż towarów lub usługi bankowości internetowej.

W przeprowadzonym badaniu skorzystano z ankiety, w której zastosowano skalę Likerta. W związku z tym w niektórych przypadkach można było wybrać jedną z następujących odpowiedzi: bardzo zaniepokojony, nieco zaniepokojony, w ogóle nie zaniepokojony bądź nie wiem. Były również pytania, na które należało odpowiedzieć „tak" bądź „nie". W związku z powyższym przeprowadzono dwutorową analizę zgromadzonych danych. Utworzone zostały dwa ich zbiory, które przed-

stawiają zupełnie skrajne sytuacje dotyczące cyberbezpieczeństwa. W pierwszym zbiorze wzięto pod uwagę zmienne od X_1 do X_6, które są destymulantami, czyli wyższe wartości wskazują, iż poziom analizowanego zjawiska, czyli sytuacji, jaka panuje w firmach odnośnie do cyberbezpieczeństwa, jest gorszy (Stanimir, 2006). W drugim rozpatrywano cechy od X_7 do X_{12}, które są stymulantami, czyli przyjmowanie wyższych wartości ma pozytywny wpływ na zjawisko, które podlega badaniu (Stanimir, 2006).

3.2. Metody analityczne zastosowane w badaniu

Na samym początku dokonano wstępnej analizy danych z wykorzystaniem statystyk opisowych. Za pomocą współczynnika zmienności określono, czy dana zmienna jest *quasi*-stałą, czy też nie. Jeżeli przyjmuje on wartość powyżej 10%, to można uznać, iż jest on istotny i dana zmienna wykazuje zróżnicowanie (Ostasiewicz i in., 2006).

W następnej kolejności dokonano analizy skupień, korzystając z klasyfikacji hierarchicznej. Pozwala ona pogrupować badane obiekty, które są homogeniczne, czyli do siebie podobne, pod względem zmiennych uwzględnionych w analizie (Kolenda, 2009, za: Prus i Król 2017). W związku z tym różnice między obiektami, które są w jednej grupie, są mniejsze niż pomiędzy obiektami pochodzącymi z różnych skupień. Aby skorzystać z tej metody, należy na samym początku znormalizować dane, np. za pomocą standaryzacji. Bardzo ważnym etapem jest utworzenie macierzy odległości pomiędzy obiektami. W celu jej sporządzenia skorzystano z odległości euklidesowej (Statsoft, b.d.). Na jej podstawie wybiera się parę obiektów, pomiędzy którymi występuje najmniejsza odległość (Balicki, 2013). To od nich rozpocznie się budowanie dendrogramu, czyli diagramu drzewa (Balicki, 2013). Finalnie otrzymuje się jedno skupienie. W celu policzenia odległości między skupieniami, które w kolejnych krokach należy połączyć, można skorzystać z następujących metod: najbliższego sąsiada, najdalszego sąsiada, mediany, centroidalnej, inaczej środka ciężkości, czy Warda (Balicki, 2013). W momencie, gdy wszystkie obiekty zostaną już połączone, należy odpowiednio podzielić diagram drzewa.

Na końcu przeprowadzono porządkowanie liniowe za pomocą ważonej metody sum standaryzowanych, która pozwala uszeregować obiekty. W wyniku tego można określić, w których z nich badane zjawisko jest lepiej oceniane, a w których gorzej. Istotną rolę odgrywa tutaj normalizacja zmiennych poprzez standaryzację oraz ujednolicenie ich charakteru. Muszą być one stymulantami. Ponadto należy pamiętać, iż wagi muszą przyjmować wartości większe od zera i sumować się do jedynki. Wyznaczone miary rozwoju należy posortować od największej do najmniejszej, ponieważ wyższe wartości wskazują na to, że zjawisko, które jest poddawane analizom, odznacza się osiąganiem wyższego poziomu (Stanimir, 2006).

4. Wyniki badań

4.1. Statystyki opisowe

Początkowo zbadano statystyki opisowe dla pierwszego zbioru zmiennych od X_1 do X_6, które znajdują się w tab. 1.

Tabela 1. Statystyki opisowe dla pierwszej grupy danych, gdzie zmienne są destymulantami

Zmienna	Liczba ważnych obserwacji	Średnia	Minimum	Maksimum	Odchylenie standardowe	Współczynnik zmienności
X_1	27	8,074	2,000	20,000	4,057	50,242
X_2	27	24,889	9,000	63,000	11,908	47,844
X_3	27	24,444	7,000	71,000	13,414	54,877
X_4	27	18,148	7,000	62,000	10,683	58,867
X_5	27	77,000	58,000	90,000	8,005	10,396
X_6	27	26,778	7,000	72,000	14,996	56,001

Źródło: opracowanie własne z wykorzystaniem programów Statistica 13 i Excel.

Na podstawie sporządzonej tab. 1 należy stwierdzić, iż nie występują braki danych oraz współczynnik zmienności dla każdej ze zmiennych jest istotny. Maksymalne wartości dla zmiennych X_2, X_3, X_4, oraz X_6 odnotowano dla Hiszpanii. W przypadku cechy X_1 maksimum zaobserwowano dla Francji, a minimum dla Estonii, w której najniższe wartości dostrzeżono także dla zmiennych: X_3 oraz X_6. Warto również wspomnieć o sytuacji w Danii, gdzie odnotowano najniższe wartości dla cech: X_2, X_3 i X_4. Zważywszy na to, że przeprowadzanie szkoleń w firmach jest istotne, warto przyjrzeć się średniej arytmetycznej dla zmiennej X_5. Jej wartość to 77%. Jest to nadal dość duży procent przedsiębiorstw. Jeśli chodzi o obawy związane z poszczególnymi cyberprzestępstwami, to średnie dla zmiennych X_2, X_3, X_4, X_6 oscylują między 18% a 26% (tab. 1). Ponadto za pomocą wykresów skrzynkowych zbadano występowanie obserwacji odstających. Dla zmiennej X_1 występuje tylko jedna obserwacja odstająca, którą jest Francja. Dla zmiennych X_2, X_3 oraz X_6 to Hiszpania jako jedyna jest obserwacją odstającą. W przypadku zmiennej X_4 występuje jedna obserwacja ekstremalna, którą jest Hiszpania. W przypadku zmiennej X_5 nie odnotowano obserwacji odstających.

Następnie wyznaczono statystyki opisowe dla drugiego zbioru zmiennych. Zostały one przedstawione w tab. 2. Na jej podstawie należy stwierdzić, iż nie występują braki danych oraz współczynnik zmienności dla każdej ze zmiennych jest istotny. Minimalne wartości dla zmiennych: X_8, X_9, X_{10}, X_{12} odnotowano dla Hiszpanii. Dla Portugalii najniższe wyniki w porównaniu z pozostałymi obiektami zaobserwowano dla zmiennych: X_7 oraz X_8. Dla cech X_8, X_9 i X_{12} maksymalne wartości, a zarazem lepsze od pozostałych analizowanych krajów stwierdzono dla Danii. Dla zmiennej X_{11} najwyższa

Tabela 2. Statystyki opisowe dla drugiej grupy danych, gdzie zmienne są stymulantami

Zmienna	Liczba ważnych obserwacji	Średnia	Minimum	Maksimum	Odchylenie standardowe	Współczynnik zmienności
X_7	27	16,111	6,000	38,000	7,165	44,471
X_8	27	29,222	9,000	45,000	8,911	30,495
X_9	27	32,556	7,000	52,000	11,026	33,867
X_{10}	27	40,000	7,000	59,000	13,229	33,072
X_{11}	27	20,556	8,000	40,000	7,366	35,834
X_{12}	27	34,407	6,000	57,000	12,401	36,042

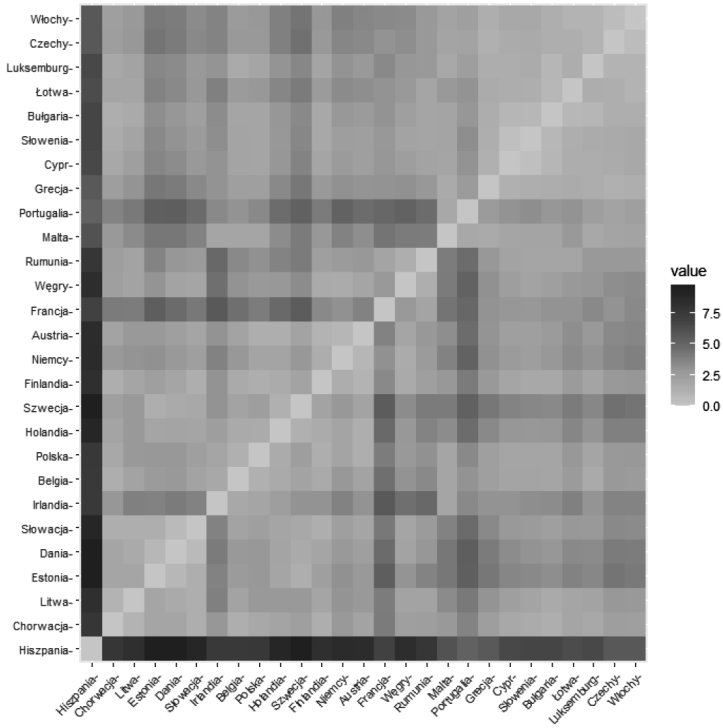
Źródło: opracowanie własne z wykorzystaniem programów Statistica 13 i Excela.

wartość dotyczyła Irlandii. Warto zwrócić uwagę na cechę X_7, która dotyczy procentu firm, w których pracownicy są bardzo dobrze poinformowani o zagrożeniach związanych z cyberprzestępczością, gdyż wartość średniej arytmetycznej jest dosyć niska i ukształtowała się na poziomie około 16%. Podobna sytuacja dotyczy przeprowadzania szkoleń, czyli zmiennej X_1, dla której średnia wyniosła około 21% (tab. 2). Na podstawie sporządzonego wykresu skrzynkowego zauważono, iż dla zmiennej X_7 występuje jedna obserwacja odstająca i jest nią Irlandia. W przypadku pozostałych zmiennych nie odnotowano obserwacji odstających.

4.2. Analiza skupień – klasyfikacja hierarchiczna

Początkowo analizę przeprowadzono dla pierwszego zbioru zmiennych od X_1 do X_6. Celem przeprowadzenia klasyfikacji hierarchicznej najpierw znormalizowano zmienne za pomocą standaryzacji. Następnie utworzono macierz odległości euklidesowych pomiędzy państwami Unii Europejskiej, która stanowi bazę wykorzystywanej metody analizy (Kassambara i Mundt, 2020) (rys. 1).

Na rysunku 1 ciemniejszy kolor świadczy o tym, że odległości między krajami są większe. Im jaśniejszy kolor, tym mniejsza odległość między obiektami, czyli istnieje między nimi większe podobieństwo. Można zauważyć, iż w zasadzie największe odległości występują pomiędzy poszczególnymi krajami a Hiszpanią. Zatem już na samym początku można wyciągnąć wniosek, iż obserwacje badanych zmiennych w Hiszpanii różnią się od pozostałych państw. Kolejnym etapem było utworzenie wykresu przebiegu aglomeracji. Umożliwia on podjęcie decyzji w kwestii wyboru odpowiedniej liczby klas, na które należałoby podzielić badane obiekty, czyli państwa. Na podstawie tego wykresu stwierdzono, iż należałoby przeciąć 23. wiązanie. Jednakże w ramach dokładniejszej analizy posłużono się także indeksem Grabińskiego i wyznaczono maksimum lokalne wskaźnika q_i, które wskazało miejsce podziału diagramu drzewa (Grabiński, 1992). Pierwsze maksimum lokalne wskaźnika q_i równe 2,019 wskazuje, iż należałoby uciąć drugie wiązanie. W wyniku tego wyłoniłoby się

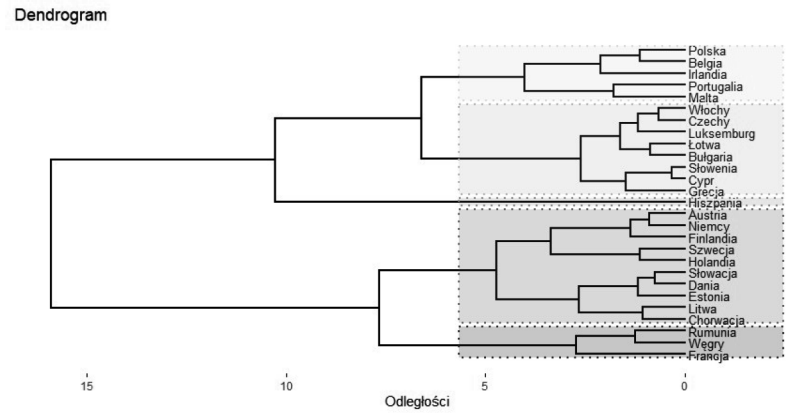


Rys. 1. Macierz odległości dla pierwszej grupy danych, gdzie zmienne są destymulantami

Źródło: opracowanie własne z wykorzystaniem programu RStudio

aż 26 grup państw. Na podstawie drugiego maksimum, które wynosi 1,545, ucięto by wiązanie 26., czyli ostatnie. Skutkowałoby to powstaniem tylko dwóch klas. Z racji tego, że dwa pierwsze maksima lokalne są skrajnymi wartościami, czyli występują dla drugiego i ostatniego wiązania, postanowiono wyznaczyć trzecie, którego wartość wynosi 1,398. Zgodnie z tym potwierdził się wniosek wyciągnięty na podstawie analizy wykresu przebiegu aglomeracji. Wobec powyższego w ostateczności dokonano podziału obiektów na 5 klas, co wiązało się z ucięciem wiązania 23. W następnej kolejności zgodnie z wyciągniętymi wcześniej wnioskami skonstruowano dendrogram, czyli diagram drzewa (Kassambara i Mundt, 2020) (rys. 2).

Zgodnie z rysunkiem 2 pierwsze skupienie to klasa jednoelementowa tworzona przez Hiszpanię. Do drugiego skupienia trafiły: Włochy, Czechy, Luksemburg, Łotwa, Bułgaria, Słowenia, Cypr oraz Grecja. W trzecim skupieniu znalazły się: Rumunia, Węgry oraz Francja. W czwartej grupie można wyróżnić następujące kraje: Polskę, Belgię, Irlandię, Portugalię oraz Maltę. Natomiast do ostatniej klasy zaliczono: Austrię, Niemcy, Finlandię, Szwecję, Holandie, Słowację, Danię, Estonię, Litwę i Chorwację (rys. 2).



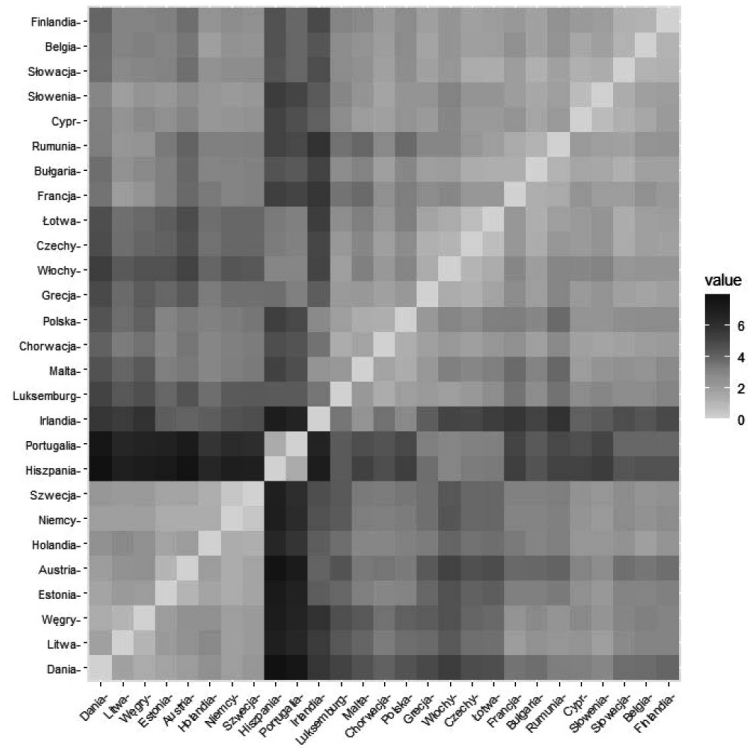
Rys. 2. Dendrogram dla pierwszej grupy danych, gdzie zmienne są destymulantami

Źródło: opracowanie własne z wykorzystaniem programu RStudio.

W celu przeprowadzenia drugiej klasyfikacji hierarchicznej opierającej się na drugim zbiorze danych dla zmiennych od X_7 do X_{12} również na samym początku znormalizowano zmienne poprzez ich standaryzację. Następnie sporządzono macierz odległości euklidesowych pomiędzy badanymi obiektami (rys. 3).

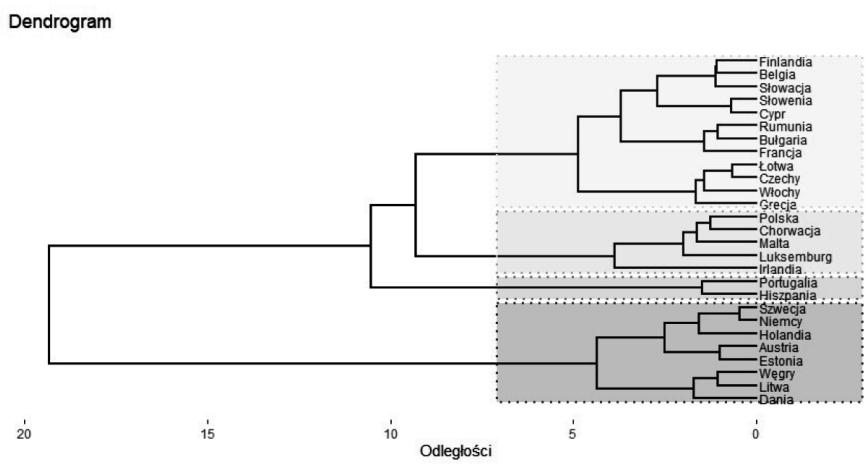
Na podstawie rysunku 3 zauważono, iż zarówno Hiszpania, jak i Portugalia są do siebie bardzo podobne, ale najmniej podobne do innych państw ze względu na badane zmienne, gdyż odległości pomiędzy nimi a pozostałymi krajami są znaczące. Wyznaczona została również najmniejsza odległość, która dotyczy Szwecji i Niemiec. Właśnie te dwa kraje zostaną jako pierwsze połączone i od nich rozpocznie się konstrukcja diagramu drzewa, czyli dendrogramu. Następną bardzo ważną kwestią było ustalenie liczby klas, na które należy podzielić państwa Unii Europejskiej. Wobec tego posłużono się wykresem przebiegu aglomeracji. W kroku 24. zauważalny był dość duży skok, jeśli chodzi o długość wiązania. Zatem zgodnie z tym wykresem można było podejrzewać, iż to w tym miejscu należałoby zakończyć łączenie diagramu drzewa. Zanim podjęto ostateczną decyzję, zbadano także indeks Grabińskiego. Pierwsze maksimum lokalne wskaźnika q_i równe 1,909 wskazuje, iż należałoby uciąć 24. wiązanie. W wyniku tego powstaną 4 klasy. Zatem zgadza się to z wnioskiem wyciągniętym na podstawie wykresu przebiegu aglomeracji. W następnej kolejności zgodnie z wyciągniętymi wcześniej wnioskami skonstruowano dendrogram, czyli diagram drzewa (Kassambara i Mundt, 2020) (rys 4).

Na rysunku 4 widać, że pierwsze skupienie tworzą Portugalia oraz Hiszpania. Do drugiej klasy należą: Polska, Chorwacja, Malta, Luksemburg i Irlandia. W trzecim skupieniu znalazły się: Szwecja, Niemcy, Holandia, Austria, Estonia, Węgry, Litwa oraz Dania. Natomiast Finlandia, Belgia, Słowacja, Słowenia, Cypr, Rumunia, Bułgaria, Francja, Łotwa, Czechy, Włochy oraz Grecja pogrupowały się razem, tworząc ostatnie ze skupień (rys. 4).



Rys. 3. Macierz odległości dla drugiej grupy danych, gdzie zmienne są stymulantami

Źródło: opracowanie własne z wykorzystaniem programu RStudio.



Rys. 4. Dendrogram dla drugiej grupy danych, gdzie zmienne są stymulantami

Źródło: opracowanie własne z wykorzystaniem programu RStudio.

W celu porównania obu przeprowadzonych klasyfikacji hierarchicznych wyznaczono współczynnik Randa. Jego wartość jest równa 0,724. Oznacza to, iż zgodność utworzonych podziałów analizowanych obiektów jest dość wysoka. Ponadto powstałe skupienia są relatywnie zbliżone do siebie. W związku z tym państwa Unii Europejskiej pogrupowały się podobnie.

4.3. Porządkowanie liniowe – ważona metoda sum standaryzowanych

Następnym krokiem niniejszego badania było skonstruowanie rankingu dla obu grup danych za pomocą metody porządkowania liniowego, jaką jest ważona metoda sum standaryzowanych. Na początku zmiennym zostały przypisane odpowiednio wagi. Zmienną, która dotyczy przeprowadzenia szkoleń i podnoszenia świadomości na temat zagrożeń związanych z cyberprzestępczością, uznano za najważniejszą w porównaniu z pozostałymi cechami. Wynika to z faktu, iż organizowanie kursów przyczynia się do tego, że pracownicy i dyrektorzy zdobywają kompetencje i poszerzają wiedzę w określonym obszarze. Zatem zmiennej tej nadano wagę równą 0,25. Cechę dotyczącą stopnia poinformowania pracowników o cyberzagrożeniach uznano za drugą co do istotności i przyznano jej wagę 0,19. Uznano, iż ma ona większe znaczenie niż pozostałe, ponieważ poinformowani pracownicy mają wiedzę na temat tego, jakie występują cyberprzestępstwa i jak w razie ich wystąpienia prawidłowo postępować. Następne cztery zmienne zostały uporządkowane na podstawie tego, ile procent małych i średnich przedsiębiorstw w Unii Europejskiej w ciągu 2021 roku doświadczyło poszczególnych cyberprzestępstw. W przypadku wirusów, *spyware* oraz *malware* odsetek ten był największy, gdyż wyniósł 14%. Natomiast na drugim miejscu znalazł się cyberatak typu phishing – z wynikiem 11%. Jeśli chodzi o *ransomware*, zjawisko to dotyczyło około 4% firm w Unii Europejskiej. Wobec powyższego zmienne dotyczące obaw związanych z wirusami, *spyware*, *malware* oraz z phishingiem otrzymały takie same wagi równe 0,17. Zmiennej, która opisuje obawy dotyczące *ransomware*, przypisano wagę 0,12. Tym samym ostatnia ze zmiennych otrzymała wagę 0,10.

Najpierw utworzono ranking na podstawie pierwszej grupy danych. Z racji tego, iż wszystkie zmienne mają charakter destymulant, przed wykonaniem porządkowania przekształcono je na stymulanty. Następnie znormalizowano zmienne za pomocą standaryzacji. W ten sposób po odpowiednich obliczeniach i uwzględnieniu wag wyznaczono miary rozwoju i uporządkowano je od największej do najmniejszej. Zgodnie z powstałym rankingiem najgorzej wypada Hiszpania. Natomiast na pierwszym miejscu plasuje się Estonia. Polska zajmuje jedenastą pozycję. Pierwsze cztery miejsca zajmują następujące państwa: Estonia, Szwecja, Dania oraz Holandia. Ponadto pogrupowały się one również razem w obu przeprowadzonych wcześniej analizach skupień.

Drugie porządkowanie dotyczyło drugiej grupy danych. W tym przypadku zmienne były stymulantami, więc zostały one najpierw zestandaryzowane. Następnie wy-

znaczono miary rozwoju. Na podstawie rankingu zauważono, iż powtórnie ostatnie miejsce zajmuje Hiszpania. Natomiast najlepiej zjawisko badane oceniono w Irlandii. Miejsca od drugiego do siódmego zajmują ponownie kraje, które znajdowały się w jednym skupieniu dla obu analiz skupień. Są to kolejno: Austria, Estonia, Dania, Niemcy, Szwecja oraz Holandia. Polska uplasowała się na dziewiątej pozycji. W porównaniu do pierwszego utworzonego rankingu znalazła się dwa miejsca wyżej.

Za pomocą współczynnika korelacji rang Spearmana zanalizowano także zależność między dwoma powstałymi rankingami. Współczynnik zawiera się w przedziale od –1 do 1 (Stanimir, 2006). Wartość tego współczynnika jest równa 0,82. Świadczy to o tym, że występuje silna korelacja i oba utworzone uporządkowania można uznać za stosunkowo zgodne.

5. Podsumowanie

Przeprowadzona analiza pozwoliła wyciągnąć wiele interesujących wniosków. Po przeprowadzeniu klasyfikacji hierarchicznych zarówno dla pierwszego, jak i drugiego zbioru danych do jednej grupy trafiły między innymi następujące państwa: Niemcy, Estonia, Szwecja, Holandia, Austria oraz Dania. Zatem potwierdziła się hipoteza, iż w jednej klasie znajdą się kraje, które zaliczane są do bogatych i bardziej rozwiniętych. Ciekawe jest to, że Estonia nie znalazła się w skupieniu z krajami Europy Środkowo-Wschodniej. W dodatku uplasowała się na pierwszym oraz trzecim miejscu w sporządzonych rankingach. Interesujący jest również fakt, iż od samego początku przeprowadzanej analizy Hiszpanię uznano za obserwację odstającą. W pierwszej klasyfikacji hierarchicznej utworzyła grupę jednoelementową, natomiast w drugiej klasyfikacji połączyła się w jedno skupienie z Portugalią. W przypadku rankingów utworzonych za pomocą ważonej metody sum standaryzowanych zauważono, iż pierwsze miejsca zajmują kraje Europy Zachodniej oraz Północnej. W związku z tym druga z hipotez również się potwierdziła i kraje te plasują się wysoko w rankingach ze względu na analizowane zmienne.

W niniejszym artykule poruszono zaledwie kilka kwestii związanych z cyberbezpieczeństwem. W związku z tym sugeruje się prowadzenie dalszych badań w celu poszerzenia wiedzy. Ważne jest też zgłębienie tematu cyberwojny i jej wpływu na państwo. Jako przykład można podać cyberataki na Ukrainę w 2017 roku oraz na Estonię w 2007 roku. Zaletą jednak jest to, że udostępniane jest coraz więcej raportów z wynikami badań na temat zarejestrowanych incydentów dotyczących cyberprzestępczości, świadomości społeczeństw w zakresie cyberbezpieczeństwa czy wydatków z nim związanych.

Literatura

Antczak, J. (2020). Costs of Cyber – Security in a Business Entity. *Education of Economists and Managers*, *55*(1), 81-93. https://doi.org/10.33119/EEiM.2020.55.6

Balicki, A. (2013). *Statystyczna analiza wielowymiarowa i jej zastosowania społeczno-ekonomiczne*. Wydawnictwo Uniwersytetu Gdańskiego.

Bambara, J. J. i Allen, P. R. (2018). *Blockchain a Practical Guide to Developing Business, Law, and Technology Solutions.* Mc Graw Hill Education.

Bay, M. (2016). What Is Cybersecurity? In Search of an Encompassing Definition for the Post – Snowden Era. *French Journal for Media Research*, (6).

Chakraborty, N. (2013). Intrusion Detection System and Intrusion Prevention System: A Comparative Study. *International Journal of Computing and Business Research*, *4*(2).

Choi, Y.B. i Allison, G. D. (2017). Intrusion Prevention and Detection in Small to Medium – Sized Enterprises. *SAIS 2017 Proceedings*, (11).

Cunningham, Ch. (2021). *Wojny w cyberprzestrzeni: koncepcje, strategie i taktyki, dzięki którym przetrwasz i ocalisz swoją organizację*. Helion.

European Commission. (2022). *Flash Eurobarometer 496 SMEs and Cybercrime – November-December 2021. Report.* (Fieldwork 26/11-17/12/2021). Pobrano 14 marca 2024 z https://europa.eu/eurobarometer/surveys/detail/2280

European Union Agency for Cybersecurity. (2021). *Cybersecurity for SMES – Challenges and Recommendations.* Pobrano 14 marca 2024 z https://www.enisa.europa.eu/publications/enisa-report-cybersecurity-for-smes

Ghosh, A. (2012, 3 maja). *Performance of Computer: What it Actually Means*. The Customize Windows. Pobrano 5 marca 2024 z https://thecustomizewindows.com/2012/05/performance-of-computer-what-it-actually-means/

Główny Urząd Statystyczny [GUS]. (2016). *Jakość życia w Polsce*. Główny Urząd Statystyczny.

Grabiński, T. (1992). *Metody taksonometrii*. Wydawnictwo Akademii Ekonomicznej w Krakowie.

Intel. (b.d.). *Ponad 50 lat prawa Moore'a.* Pobrano 24 października 2022 z https://www.intel.pl/content/www/pl/pl/innovation/leadership/overview.html

JEL Classification System. (2023.) Pobrano 10 maja 2024 https://www.aeaweb.org/econlit/jelCodes.php#:~:text=EconLit%

Kassambara, A. i Mundt, F. (2020). *Extract and Visualize the Results of Multivariate Data Analyses – Package Factoextra.* Pobrano z https://cran.r-project.org/web/packages/factoextra/factoextra.pdf

Mathew, A. R. (2019). Cyber Security through Blockchain Technology. *International Journal of Engineering and Advanced Technology*, *9*(1), 3821-3824, https://doi.org/10.35940/ijeat.A9836.109119

Ostasiewicz, S., Rusnak, Z. i Siedlecka, U. (2006). *Statystyka elementy teorii i zadania*. Wydawnictwo Akademii Ekonomicznej im. Oskara Langego we Wrocławiu.

Prus, B. i Król, K. (2017). Ocena zastosowania wybranych metod taksonomicznych do klasyfikacji zjawisk społeczno-gospodarczych. *Acta Scientiarum Polonorum Formatio Circumiectus*, *16*(2), 179-197. Pobrano z https://acta.urk.edu.pl/pdf-102528-34000?filename=OCENA%20ZASTOSOWANIA.pdf

Stanimir, A. (red.). (2006). *Analiza danych marketingowych*. Wydawnictwo Akademii Ekonomicznej im. Oskara Langego we Wrocławiu.

StatSoft. (b.d.). *Analiza skupień*. Pobrano 2 stycznia 2024 z https://www.statsoft.pl/textbook/stathome_stat.html?https%3A%2F%2Fwww.statsoft.pl%2Ftextbook%2Fstcluan.html.

Szafranek, D. (2021). Wpływ rozwoju cyberprzestępczości na funkcjonowanie współczesnych organizacji. *Nowoczesne Systemy Zarządzania*, *16*(4), 43-54, DOI: http://dx.doi.org/10.37055/nsz/147080.

Research on the Level of Implementation of Cybersecurity Objectives of European Union Companies and Institutions

Abstract: Cybersecurity is a very important topic that is being talked about and heard more and more often. It has gained importance with technological development. The aim of the article is to examine the situation in the area of cybersecurity in small- and medium-sized enterprises in the European Union and to discuss the forms of protecting companies against cyber threats. For this purpose, a two--way analysis was carried out using hierarchical classification and linear ordering using the standardised sum method. The data comes from a study conducted by Ipsos European Public Affairs. The analysis and the resulting conclusions confirmed the hypotheses that richer and more developed countries would be grouped together and that Western and Northern European countries would rank high in the rankings.

Keywords: cybersecurity, cybercrime, blockchain, hierarchical classification, linear ordering