1. Sławomir Andrzej TORBUS[1], 2. Dawid KOLANO, 3. Adam KUCZKOWSKI, 4. Mateusz WERYHO

Uniwersytet Kazimierza Wielkiego, Instytut Matematyki (1)
ORCID: 1. 0000-0002-1594-6953

doi:10.15199/48.2025.01.14

Zastosowanie wybranych metod korelacji do analizy zjawisk zachodzących w systemach bezpieczeństwa informacyjnego

Streszczenie. *W części teoretycznej pracy omówiono wybrane metody korelacyjne (współczynnik korelacji liniowej Pearsona, diagram rozrzutu, nożyce korelacji, regresja liniowa), które należy stosować podczas analizy zjawisk zachodzących w systemach bezpieczeństwa informacyjnego. W części praktycznej pracy zaprezentowano przykładową analizę korelacyjną (metodami analitycznymi i graficznymi) rzeczywistych danych (nakładów finansowych na poziom cyberbezpieczeństwa w RP oraz liczby oszustw komputerowych zgłaszanych do CERT Polska przez obywateli RP). Na podstawie uzyskanych wyników sformułowano wnioski dotyczące zależności pomiędzy rozpatrywanymi danymi za lata 2018 – 2023.*

Abstract. *The theoretical part of the work discusses the selected correlation methods (Pearson's linear correlation coefficient, scatter diagram, correlation scissors, linear regression), which should be used for analyze phenomena occurring in systems of information security. The practical part of the work presents an example of a correlation analysis (using analytical and graphical methods) of the real data (financial outlays on the level of cybersecurity in the Republic of Poland and the number of computer frauds reported to CERT Polska by citizens of the Republic of Poland). On the basis of the obtained results, conclusions were formulated regarding the relationship between the data considered for the years 2018 – 2023. (**Application of selected correlation methods for analyze phenomena occurring in systems of information security**)*

Słowa kluczowe: analiza korelacyjna, współczynnik korelacji liniowej Pearsona, diagram rozrzutu, nożyce korelacji, regresja liniowa, cyberbezpieczeństwo, system bezpieczeństwa informacyjnego
Keywords: correlation analysis, Pearson's linear correlation coefficient, scatter diagram, correlation scissors, linear regression, cybersecurity, information security system

Wstęp

Cyberbezpieczeństwo ma na celu ochronę danych i systemów wewnętrznych przed zagrożeniami, jakie niosą za sobą cyberataki. Oznacza to, że mieszczą się w nim nie tylko technologie, ale także procesy, które kontrolują i chronią sieć, oprogramowanie oraz urządzenia. Efektem takich działań jest zmniejszenie ryzyka cyberataków oraz skuteczna ochrona przed nieuprawnionym wykorzystaniem danych i oprogramowania, co czyni system informatyczny odpornym na działania naruszające poufność (dane dostępne są tylko dla uprawnionych osób), integralność (dane są dokładne i niezmienione), dostępność (dane są dostępne dla uprawnionych osób, gdy ich potrzebują) i autentyczność (dane są w rzeczywistości tym, czym się wydają) [1].

W Rzeczypospolitej Polskiej podstawowym aktem prawnym w zakresie cyberbezpieczeństwa jest Ustawa z dnia 5 lipca 2018 roku o krajowym systemie cyberbezpieczeństwa (Dz.U. 2018 poz. 1560) [2], która obowiązuje do dnia dzisiejszego. Zapewnia ona ochronę cyberprzestrzeni na poziomie krajowym i gwarantuje między innymi niezakłócone świadczenie usług kluczowych z punktu widzenia państwa i gospodarki oraz usług cyfrowych poprzez osiągnięcie wysokiego poziomu bezpieczeństwa systemów informatycznych służących do ich świadczenia [1,2].

Tabela 1. Nakłady finansowe na poziom cyberbezpieczeństwa w RP oraz liczba oszustw komputerowych zgłaszanych do CERT Polska przez obywateli RP [3]

Rok	Nakłady finansowe na poziom cyberbezpieczeństwa w RP [mld PLN]	Liczba oszustw komputerowych zgłaszanych do CERT Polska przez obywateli RP
2018	1,4	1878
2019	1,6	4086
2020	1,7	8310
2021	1,9	17525
2022	2,1	28742
2023	2,4	80267

Cyberbezpieczeństwo jest niezwykle istotne z punktu widzenia różnego typu organizacji i przedsiębiorstw, jak i osób prywatnych, ponieważ jedni jak i drudzy operują na różnego typu danych. Jest więc bardzo ważne zarówno dla sektora publicznego, jak i prywatnego. Wobec powyższego wdrażane są procedury związane z cyberbezpieczeństwem, a co za tym idzie ponoszone są odpowiednio duże nakłady finansowe (Tabela 1.), aby zagwarantować odpowiedni poziom bezpieczeństwa (danych, szeroko rozumianych systemów IT, różnego typu oprogramowania), który dotyczy [5,6,7,8]:

- ochrony przed utratą danych wrażliwych,
- zapobiegania stratom finansowym, które często są wynikiem cyberataków oraz awarii powodujących przestoje w funkcjonowaniu przedsiębiorstwa,
- zapobiegania utracie reputacji, która zwykle jest skutkiem nieodpowiedniego dbania o zabezpieczenie danych.

Omawiając zagadnienie cyberbezpieczeństwa należy wspomnieć o najczęściej występujących oszustwach komputerowych zgłaszanych do CERT (ang. Computer Emergency Response Team) Polska przez obywateli RP. Są nimi [5,6,7]:

- phishing – podszywanie się pod inną osobę lub instytucję w celu nakłonienia użytkownika do podania poufnych informacji, takich jak hasła lub dane osobowe,
- malware – złośliwe oprogramowanie, które może uszkodzić systemy informatyczne lub wykraść dane. Przykładem są wirusy, trojany, robaki i ransomware,
- ataki typu DDoS – przeciążenie serwera dużą ilością żądań, co uniemożliwia jego działanie,
- inżynieria społeczna – manipulowanie ludźmi w celu skłonienia ich do ujawnienia poufnych informacji lub wykonania niebezpiecznych czynności,
- ataki typu zero-day – wykorzystanie luk bezpieczeństwa w oprogramowaniu, które nie są jeszcze znane producentowi.

CERT znajduje się w grupie Zespołów Reagowania na Incydenty Komputerowe i stanowią go specjaliści, którzy zajmują się [3,7]:

- reagowaniem na incydenty z obszaru bezpieczeństwa informatycznego tzn. pomocą osobom i organizacjom, które padły ofiarą ataków hackerskich lub innych incydentów bezpieczeństwa,
- monitorowaniem cyberprzestrzeni w poszukiwaniu nowych zagrożeń i ostrzeganiem użytkowników przed nimi oraz ich negatywnymi skutkami,
- wymianą, między krajowymi zespołami CERT, informacji o zagrożeniach i najlepszych praktykach walki z nimi,
- prowadzeniem szkoleń i innych działań edukacyjnych dla użytkowników na temat bezpieczeństwa szeroko rozumianego sektora IT.

Zespół CERT Polska funkcjonuje od 1996 roku i jest umiejscowiony w Pionie Centrum Cyberbezpieczeństwa NASK-PIB (Naukowa i Akademicka Sieć Komputerowa – Państwowy Instytut Badawczy), który jest państwowym instytutem badawczym nadzorowanym przez Ministerstwo Cyfryzacji. Jako samodzielna jednostka badawczo-rozwojowa funkcjonuje od 1993 roku, a więc w 2023 roku obchodziła trzydziestolecie swej działalności [3,4].

Zgodnie z Ustawą z dnia 5 lipca 2018 roku o krajowym systemie cyberbezpieczeństwa NASK-PIB został wskazany jako jeden z Zespołów Reagowania na Incydenty Komputerowe [4], który koordynuje obsługę incydentów zgłaszanych przez operatorów usług kluczowych, dostawców usług cyfrowych, samorząd terytorialny. Do NASK-PIB incydenty mogą także zgłaszać wszyscy użytkownicy. NASK-PIB współtworzy także zaplecze analityczne oraz badawczo-rozwoje dla krajowego systemu cyberbezpieczeństwa.

Analizując dane zawarte w Tabeli 1 można zauważyć coroczny wzrost liczby oszustw komputerowych zgłaszanych do CERT Polska przez obywateli RP. Na szczególną uwagę zasługuje rok 2020, w którym rozpoczęła się pandemia COVID-19 wywołana przez koronawirusa SARS-COV-2 oraz rok 2022, w którym rozpoczęła się inwazja Rosji na Ukrainę, problemy na granicy z Białorusią oraz ataki hybrydowe. W tych latach wzrost liczby oszustw komputerowych zgłaszanych do CERT Polska przez obywateli RP stał się szczególnie zauważalny i to właśnie stało się asumptem do przeprowadzenia analizy korelacyjnej umożliwiającej określenie zależności pomiędzy nakładami finansowymi na poziom cyberbezpieczeństwa w RP a liczbą oszustw komputerowych zgłaszanych do CERT Polska przez obywateli RP oraz do sformułowania wniosków dotyczących wpływu nakładów finansowych instytucji rządowych i pozarządowych na poziom cyberbezpieczeństwa w RP, w latach 2018 – 2023, to jest od momentu wejścia w życie Ustawy z dnia 5 lipca 2018 roku o krajowym systemie cyberbezpieczeństwa. Dodatkowo warto zaznaczyć, że właśnie w 2023 roku minęło pełne 5 lat od jej wejścia w życie, co skłania do podjęcia tematu dotyczącego analizy z wykorzystaniem metod korelacji prawidłowości jej realizowania przez instytucje rządowe i pozarządowe.

Charakterystyka i zastosowanie analitycznej metody badania korelacji pomiędzy nakładami finansowymi na poziom cyberbezpieczeństwa w RP a liczbą oszustw komputerowych z wykorzystaniem współczynnik korelacji liniowej Pearsona

Do analitycznego badania zależności korelacyjnej często stosuje się współczynnik korelacji liniowej Pearsona, zdefiniowany jako iloraz kowariancji i iloczynu odchyleń standardowych dyskretnych zmiennych losowych X i Y [10].

W praktyce, podczas korelacyjnej analizy danych, dla których trudno jest określić prawdopodobieństwo ich występowania, korzysta się z estymatora współczynnika korelacji liniowej Pearsona, opisanego wzorem [10]:

$$r_{XY} = \frac{\sum_{i=1}^{n}\left(x_i - m_X\right)\cdot\left(y_i - m_Y\right)}{\sqrt{\sum_{i=1}^{n}\left(x_i - m_X\right)^2}\cdot\sqrt{\sum_{i=1}^{n}\left(y_i - m_Y\right)^2}} \quad (1)$$

gdzie: m_X – średnia arytmetyczna z elementów zmiennej losowej X, m_Y – średnia arytmetyczna z elementów zmiennej losowej Y, x_i – element zmiennej losowej X, y_i – element zmiennej losowej Y (i = 1, 2, 3, …).

Współczynnik korelacji liniowej Pearsona oraz jego estymata przyjmują wartości z przedziału [-1;1]. Jeżeli współczynnik korelacji bądź jego estymata przyjmuje wartość -1 lub +1, to między zmiennymi losowymi X i Y istnieje ścisła zależność w postaci funkcji liniowej (zmienne losowe są w pełni skorelowane). Jeżeli przyjmuje wartość 0, wówczas zmienne losowe X i Y nie są skorelowane (nie ma między nimi żadnej zależności). Im wartość bezwzględna współczynnika korelacji bądź jego estymata jest bliższa jedności, tym mocniejsza jest korelacja pomiędzy zmiennymi losowymi X i Y.

Tabela 2. Sposób interpretacji stopnia skorelowania zmiennych losowych na podstawie wartość współczynnika korelacji liniowej Pearsona bądź jego estymaty [11]

Wartość współczynnika korelacji liniowej Pearsona bądź jego estymaty	Sposób interpretacji stopnia skorelowania zmiennych losowych
$\|r_{XY}\| < 0{,}2$	brak związku liniowego
$0{,}2 \le \|r_{XY}\| < 0{,}4$	słaba zależność
$0{,}4 \le \|r_{XY}\| < 0{,}7$	umiarkowana zależność
$0{,}7 \le \|r_{XY}\| < 0{,}9$	dość silna zależność
$\|r_{XY}\| \ge 0{,}9$	bardzo silna zależność

W celu ułatwienia interpretowania stopnia skorelowania zmiennych losowych sformułowano w pracy [11] progi dla wartości współczynnika korelacji liniowej Pearsona bądź jego estymaty i przypisano im stopnie zależności między zmiennymi losowymi (Tabela 2.).

Na podstawie danych zawartych w Tabeli 1., przy użyciu arkusza kalkulacyjnego, wyznaczono wartości parametrów statystycznych (średnich arytmetycznych i odchyleń standardowych) dyskretnych zmiennych losowych oraz estymatę współczynnika korelacji liniowej Pearsona, które zawarto w Tabeli 3.

Tabela 3. Wartości parametrów statystycznych dyskretnych zmiennych losowych oraz estymata współczynnika korelacji liniowej Pearsona

Obliczany parametr	Wartość obliczanego parametru
Średnia arytmetyczna nakładów finansowych na poziom cyberbezpieczeństwa w RP	$m_X = 1{,}9$
Średnia arytmetyczna liczby oszustw komputerowych zgłaszanych do CERT Polska przez obywateli RP	$m_Y = 23468$
Odchylenie standardowe nakładów finansowych na poziom cyberbezpieczeństwa w RP	$\sigma_X = 0{,}4$
Odchylenie standardowe liczby oszustw komputerowych zgłaszanych do CERT Polska przez obywateli RP	$\sigma_Y = 29532$
Estymata współczynnika korelacji liniowej Pearsona	$r_{XY} = 0{,}9$

Współczynnik korelacji liniowej Pearsona ma wartość 0,9. Na tej podstawie można stwierdzić, że w latach 2018 – 2023 między liczbą oszustw komputerowych zgłoszonych do CERT Polska przez obywateli RP a nakładami finansowymi na poziom cyberbezpieczeństwa w RP

występowała dodatnia i bardzo silna zależność. Oznacza to, że wzrost liczby oszustw komputerowych determinował wzrost nakładów finansowych instytucji rządowych i pozarządowych na poziom cyberbezpieczeństwa w RP.

Charakterystyka i zastosowanie wybranych graficznych metod badania korelacji pomiędzy nakładami finansowymi na poziom cyberbezpieczeństwa w RP a liczbą oszustw komputerowych

Zamieszczone w Tabeli 1. dane można potraktować jako dwie zmienne losowe dyskretne [9,10]: *X* – nakłady finansowe na poziom cyberbezpieczeństwa w RP, *Y* – liczba oszustw komputerowych zgłaszanych do CERT Polska przez obywateli RP.

Zależność między dyskretnymi zmiennymi losowymi bada się graficznymi metodami analizy korelacyjnej. Najczęściej stosowanymi są [9,11]:

- korelacyjny diagram rozrzutu (wykres rozrzutu, wykres korelacji): zbiór punktów na płaszczyźnie, które odpowiadają uporządkowanym parom liczb (*x*, *y*), gdzie: *x*, *y* – obserwacje niezależnych dyskretnych zmiennych losowych *X*, *Y*. W przypadku tej metody zakłada się, że dwuwymiarowy rozkład badanych cech zmiennych losowych *X* i *Y* jest normalny lub zbliżony do normalnego. Należy podkreślić, że diagram rozrzutu nie bada związku przyczynowo-skutkowego zachodzącego między zmiennymi losowymi, lecz związek korelacyjny. Na jego podstawie, dokonując wzrokowej oceny, można określić rodzaj zależności (korelację dodatnią, ujemną, liniową, krzywoliniową),
- nożyce korelacji: proste w kartezjańskim układzie współrzędnych, na podstawie których można określić stopień skorelowania dyskretnych zmiennych losowych *X* i *Y*. Opisują je równania:

$$x = m_X + r_{XY} \cdot \frac{\sigma_X}{\sigma_Y} \cdot \left(y - m_Y \right) \tag{2}$$

$$y = m_Y + r_{XY} \cdot \frac{\sigma_Y}{\sigma_X} \cdot \left(x - m_X \right) \tag{3}$$

gdzie: m_X – średnia arytmetyczna z elementów zmiennej losowej *X*, m_Y – średnia arytmetyczna z elementów zmiennej losowej *Y*, r_{XY} – współczynnik korelacji liniowej Pearsona, σ_X – odchylenie standardowe zmiennej losowej *X*, σ_Y – odchylenie standardowe zmiennej losowej *Y*. Na ich podstawie można określić rodzaj oraz siłę zależności (brak korelacji, korelację umiarkowaną bądź silną),

- regresja liniowa: prosta regresji oraz punkty o współrzędnych (*x*, *y*), gdzie: *x*, *y* – obserwacje niezależnych dyskretnych zmiennych losowych *X*, *Y*, w kartezjańskim układzie współrzędnych. Na podstawie rozkładu punktów względem prostej regresji można wnioskować o kierunku i sile związku korelacyjnego między dyskretnymi zmiennymi losowymi *X* i *Y*. Wyróżnia się następujące związki:
  - gdy punkty badanej korelacji grupują się wzdłuż hipotetycznej prostej nazywanej prostą regresji, przyjmując kształt zbliżony do „cygara”, świadczy to o znacznej sile związku,
  - duża ilość punktów odstających od tej prostej, przyjmujących łącznie kształt mniej lub bardziej regularnej „chmury”, świadczy o słabości badanego związku, gdy wraz ze wzrostem wartości cechy niezależnej następuje wzrost wartości zmiennej zależnej mówimy o związku wprost proporcjonalnym, a w przeciwnym wypadku, mamy do czynienia z zależnością odwrotnie proporcjonalną.

Zakładając, że znane są wartości niezależnej dyskretnej zmiennej losowej *X*, natomiast wartości dyskretnej zmiennej zależnej *Y* są nieznanymi wartościami, to ich średnie wartości spełniają równanie, nazywane równaniem prostej regresji i opisane zależnością:

$$y = a \cdot x + b \tag{4}$$

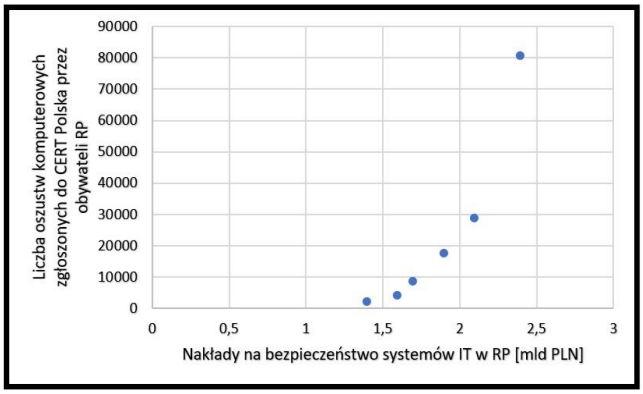
Równanie prostej regresji należy tak wymodelować, aby było najlepiej dopasowane do danych empirycznych. Współczynniki (*a* – kierunkowy i *b* – przesunięcia) prostej regresji są zwykle szacowane metodą najmniejszych kwadratów, w której suma kwadratów odchyleń rzędnych punktów empirycznych od wykresu prostej regresji była najmniejsza. W myśl teorii jest to kryterium mocne, ponieważ sumowane są kwadraty odchyleń, a więc liczby nieujemne. Współczynnik kierunkowy prostej regresji oblicza się ze wzoru:

$$a = \frac{\sum_{i=1}^{n} x_i \cdot y_i - m_X \cdot m_Y}{\sum_{i=1}^{n} x_i^2 - n \cdot m_X^2} = \frac{\sum_{i=1}^{n} x_i \cdot y_i - \frac{1}{n^2} \cdot \sum_{i=1}^{n} x_i \cdot \sum_{i=1}^{n} y_i}{\sum_{i=1}^{n} x_i^2 - n \cdot \left(\frac{1}{n} \sum_{i=1}^{n} x_i \right)^2} \tag{5}$$

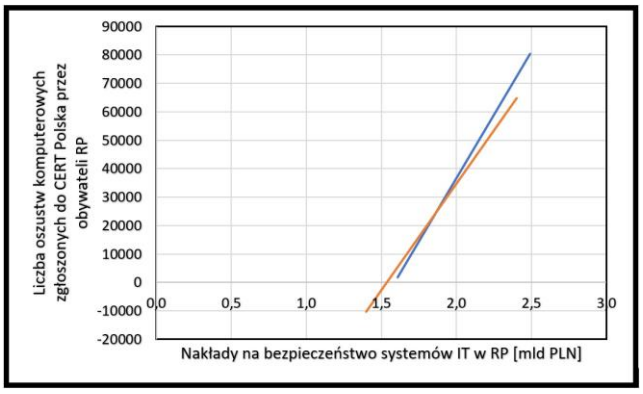
gdzie: m_X – średnia arytmetyczna z elementów zmiennej losowej *X*, m_Y – średnia arytmetyczna z elementów zmiennej losowej *Y* x_i – element zmiennej losowej *X*, y_i – element zmiennej losowej *Y* (i = 1, 2, 3, …).
Współczynnik przesunięcia prostej regresji szacuje się na podstawie próbkowego oszacowania średnich wartości w populacjach X i Y korzystając ze wzoru:

$$b = \bar{y} - a \cdot \bar{x} = \frac{1}{n} \cdot \sum_{i=1}^{n} y_i - a \cdot \frac{1}{n} \cdot \sum_{i=1}^{n} x_i \tag{6}$$

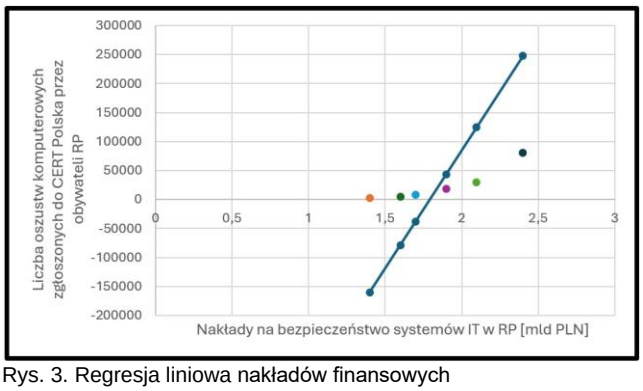
- Interpretacja współczynnika kierunkowego prostej regresji jest następująca: $a > 0$ – jeżeli *x* wzrośnie o 1 jednostkę, to *y* wzrośnie średnio o *a* jednostek; $a < 0$ – jeżeli *x* wzrośnie o 1 jednostkę, to *y* zmaleje średnio o *a* jednostek.



Rys. 1. Korelacyjny diagram rozrzutu nakładów finansowych na poziom cyberbezpieczeństwa w RP oraz liczby oszustw komputerowych zgłaszanych do CERT Polska przez obywateli RP



Rys. 2. Nożyce korelacji nakładów finansowych na poziom cyberbezpieczeństwa w RP oraz liczby oszustw komputerowych zgłaszanych do CERT Polska przez obywateli RP



Rys. 3. Regresja liniowa nakładów finansowych na poziom cyberbezpieczeństwa w RP oraz liczby oszustw komputerowych zgłaszanych do CERT Polska przez obywateli RP

Tabela 4. Równania prostych tworzących nożyce korelacji oraz równanie prostej regresji

Równania prostych tworzących nożyce korelacji	$x = 0,00001 \cdot y + 1,6$ $y = 74955 \cdot x - 115199$
Równanie prostej regresji	$y = 406373 \cdot x - 728323$

Korzystając z danych zawartych w Tabeli 1. oraz arkusza kalkulacyjnego, wyznaczono korelacyjny diagram rozrzutu (Rys. 1.). Następnie, korzystając z danych zawartych w Tabelach 1. i 2., wyznaczono równania prostych tworzących nożyce korelacji oraz równanie prostej regresji, które zawarto w Tabeli 4. i na ich podstawie, w arkuszu kalkulacyjnym, sporządzono wykresy nożyc korelacji (Rys. 2.) oraz regresji liniowej (Rys. 3.). Sformułowano wnioski szczegółowe dotyczące zależności między analizowanymi dyskretnymi zmiennymi losowymi (nakładami finansowymi na poziom cyberbezpieczeństwa w RP oraz liczbą oszustw komputerowych zgłoszonych do CERT Polska przez obywateli RP w latach 2018 – 2023):

- na podstawie korelacyjnego diagramu rozrzutu można stwierdzić, że występowała dodatnia korelacja krzywoliniowa, jednak nie można określić jej siły,
- na podstawie nożyc korelacji można stwierdzić, że występowała dodatnia i bardzo silna korelacja. Wynika to z faktu, że obydwie proste charakteryzują się dodatnimi współczynnikami kierunkowymi, a kąt zawarty między nimi jest bliski 0° (proste prawie pokrywają się),
- na podstawie regresji liniowej można stwierdzić, że występowała dodatnia korelacja, ponieważ prosta regresji ma dodatni współczynnik kierunkowy. Dodatkowo większość punktów skupia się wokół prostej regresji, co można zinterpretować jako umiarkowaną, a nawet dość silną zależność. Należy jednak dodać, że w tym przypadku metoda ta może dać zafałszowany wynik, gdyż rozpatrywana jest mała liczba danych, to jest jedynie tylko 6 par.

Wnioski

Niniejsza praca zawiera zestawienie wyników analiz statystycznych dotyczących wpływu nakładów finansowych instytucji rządowych i pozarządowych na poziom cyberbezpieczeństwa w RP, w latach 2018 – 2023. Na ich podstawie można sformułować następujące konkluzje:

- każda z metod pokazała, że mamy do czynienia z korelacją dodatnią, co oznacza, że wzrost liczby oszustw komputerowych zgłoszonych do CERT Polska przez obywateli RP determinował wzrost nakładów finansowych instytucji rządowych i pozarządowych na poziom cyberbezpieczeństwa w RP,
- zarówno metoda analityczna (współczynnik korelacji liniowej Pearsona) jak i metody graficzne (nożyce korelacji, regresja liniowa) wskazały na silną zależność. Oznacza to, że prawidłowo prognozowano nakłady finansowe na cyberbezpieczeństwo, aby zapobiegać oszustwom komputerowym bądź niwelować ich negatywne skutki. Wysokość środków finansowych była adekwatna, a ich przyrost rok do roku wystarczający.

Warto podkreślić, że w obydwu zmiennych losowych (nakładach finansowych na poziom cyberbezpieczeństwa w RP oraz liczbie oszustw komputerowych zgłaszanych do CERT Polska przez obywateli RP) każda wartość jest wartością modalną (modą) natomiast wartości środkowe (mediany) mają odpowiednio wartości 1,8 mld PLN oraz 12918. W obydwu przypadkach miary tendencji centralnej (wartość średnia, mediana i moda) nie są sobie równe, oznacza to, że obydwie zmienne losowe mają skośny rozkład danych.

Autorzy: *dr inż. Sławomir Andrzej Torbus, prof. uczelni, Uniwersytet Kazimierza Wielkiego w Bydgoszczy, Instytut Matematyki, al. Powstańców Wielkopolskich 2, 85-090 Bydgoszcz, E-mail: slawomir.torbus@ukw.edu.pl; Dawid Kolano, E-mail: dawid.kolano@student.ukw.edu.pl; Adam Kuczkowski, E-mail: adam.kuczkowski@student.ukw.edu.pl; Mateusz Weryho, E-mail: mateusz.weryho@student.ukw.edu.pl;*

LITERATURA

[1] Krawiec J., Cyberbezpieczeństwo: podejście systemowe, Oficyna Wydawnicza Politechniki Warszawskiej, Warszawa (2019)
[2] https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20180001560
[3] https://cert.pl/
[4] https://www.nask.pl/
[5] Barczak A., Sydoruk T., Bezpieczeństwo systemów informatycznych, Wydawnictwo Akademii Podlaskiej, Siedlce (2002)
[6] Janczak J., Nowak A., Bezpieczeństwo informacyjne: wybrane problemy, Akademia Obrony Narodowej, Warszawa (2013)
[7] Kowalewski J., Kowalewski M., Polityka bezpieczeństwa informacji w praktyce, Presscom, Wrocław (2014)
[8] Stallings W., Brown L., Bezpieczeństwo systemów informatycznych: zasady i praktyka, Tom 1 i Tom 2, Helion, Warszawa (2019)
[9] Sobczak M., Statystyka, PWN, Warszawa (2022)
[10] Gerstenkorn T., Środka T., Kombinatoryka i rachunek prawdopodobieństwa, PWN, Warszawa (1980)
[11] Cohen J., Statistical Power Analysis for the Behavioral Sciences, Routledge, New York (1988)