Uniwersytet Kaliski
im. Prezydenta Stanisława Wojciechowskiego
RADA NAUKOWA DYSCYPLINY NAUK O BEZPIECZEŃSTWIE

Rozprawa doktorska

Bezpieczeństwo systemu informacyjnego organizacji publicznej na przykładzie uczelni wyższej

mgr Agnieszka Gajewska

Promotor:
prof. dr hab. inż. Jarosław Wołejszo
Promotor pomocniczy:
dr Zuzanna Przyłuska

KALISZ, 2024

Serdeczne podziękowania kieruję w stronę Promotora
Pana prof. dra hab. inż. Jarosławowa Wołejszo
za wsparcie, życzliwość i nieocenioną pomoc
podczas realizacji planów naukowych.
Dziękuję także Promotorowi pomocniczemu *Pani dr Zuzannie Przyłuskiej*
Składam podziękowania Władzom Uczelni
za umożliwienie przeprowadzenia badań empirycznych
oraz Panu *Dyrektorowi, w którym miałam ogromne wsparcie* i zrozumienie.
W sposób szczególny dziękuję Rodzinie *za wyrozumiałość i cierpliwość*.

SPIS TREŚCI

Streszczenie 5

WSTĘP 10

METODOLOGIA BADAŃ WŁASNYCH 14

1.1.Uzasadnienie wyboru tematu 14

1.2. Przedmiot badań i cele badawcze 15

1.3. Problem badawczy 16

1.4. Hipotezy robocze 16

1.5. Metody, techniki, narzędzia badawcze 19

1.6. Dobór i charakterystyka próby badawczej 27

1.7. Ogólna charakterystyka terenu badań 39

1.8. Charakterystyka procedury badawczej, w tym wskazanie etapów i harmonogramu pracy badawczej 40

2. BEZPIECZEŃSTWO SYSTEMU INFORMACYJNEGO 43

2.1. Istota bezpieczeństwa systemu informacyjnego 45

2.2. Znaczenie informacji, funkcje, narzędzia służące do jej oceny 47

2.3. Znaczenie bezpieczeństwa systemu informacyjnego 58

2.4. Znaczenie bezpieczeństwa systemu informacyjnego dla bezpieczeństwa narodowego . 74

2.5. Źródła prawa dotyczące bezpieczeństwa informacyjnego 79

2.6. Diagnoza systemu informacyjnego w uczelni wyższej 82

Wnioski 122

3. ZAGROŻENIA BEZPIECZEŃSTWA SYSTEMU INFORMACYJNEGO 124

3.1.Wyzwania i zagrożenia bezpieczeństwa systemu informacyjnego 127

3.2. Aspekty bezpieczeństwa systemu informacyjnego – strategia 147

3.3. Standardy i normy bezpieczeństwa systemu informacyjnego 151

w uczelni wyższej 151

3.4. Charakterystyka zagrożeń i ograniczeń bezpieczeństwa systemu informacyjnego w uczelni wyższej 155

Wnioski 299

4. KONCEPCJA BEZPIECZEŃSTWA SYSTEMU INFORMACYJNEGO 302

4.1. Zmiany w organizacji systemu informacyjnego 304

4.2. Zmiany w obszarze bezpieczeństwa systemu informacyjnego w uczelni wyższej 368

ZAKOŃCZENIE 385

BIBLIOGRAFIA 389

SPIS RYSUNKÓW 399

SPIS TABEL 400

SPIS WYKRESÓW 407
Wykaz załączników 420

Streszczenie

Niniejsza Dysertacja pt. *Bezpieczeństwo systemu informacyjnego organizacji publicznej na przykładzie uczelni wyższej* miała na celu ocenę systemu informacyjnego funkcjonującego w uczelni wyższej. Współczesne społeczeństwo nakierowane jest na przemiany związane z wykorzystaniem technologii cyfrowych. Została dokonana weryfikacja bezpieczeństwa systemu informacyjnego z uwzględnieniem specyfiki organizacji, jaką jest publiczna uczelnia wyższa. Badaniom zostało poddane wewnętrzne środowisko użytkowników, które charakteryzuje się zróżnicowaną strukturą nakierowaną na działalność jednostki związaną z kształceniem studentów, zatrudnieniem pracowników oraz działalnością naukową.

Głównym powodem do napisania dysertacji był brak oceny bezpieczeństwa systemu informacyjnego w uczelni wyższej, który w wyczerpujący sposób wskazywałby źródła zagrożeń oraz nakreślał kierunki, sposoby implementacji zmian w badanym obszarze. Ze względu na nowe horyzonty poznawcze wynikające z przemyśleń autorki w połączeniu z analizą literatury przedmiotu oraz materiału empirycznego i ze względu na chęć ukazania koncepcji zmian w obszarze bezpieczeństwa systemu informacyjnego rozprawa doktorska wpisuje się w nauki o bezpieczeństwie.

W dysertacji zostały szeroko omówione zagrożenia bezpieczeństwa systemu informacyjnego, które obecnie nie są w pełni rozpoznawalne jak również nie można przewidzieć rozległości ich szkodliwego działania. W społeczności akademickiej jak i wśród ogółu społeczności widoczna jest niska świadomość istoty zagrożenia bezpieczeństwa systemu informacyjnego. Możliwość poznania od wewnątrz środowiska akademickiego pozwoliło autorce na zdefiniowanie obszarów problemowych, które przyczyniły się do oceny poziomu bezpieczeństwa systemu informacyjnego w uczelni wyższej. Struktura rozprawy doktorskiej obejmuje dwie części a mianowicie, cześć teoretyczną i empiryczną.

Dysertacja składa się ze wstępu, czterech rozdziałów, zakończenia, bibliografii, spisu rysunków, spisu tabel, spisu wykresów oraz załączników takich jak, kwestionariusz ankiety, kwestionariusz wywiadu z ekspertami wraz ze sprawozdaniem i arkusz obserwacji. W celu weryfikacji postawionych hipotez w drugim, trzecim, czwartym rozdziale został obliczony współczynnik korelacji liniowej Pearsona oraz współczynnik determinacji.

W rozdziale pierwszym mającym tytuł *Metodologia badań własnych*, zostały poruszone kwestie odnoszące się do przedmiotu i celu badań naukowych. Wskazany został problem badawczy, hipotezy robocze i hipotezy szczegółowe. Omówione zostały metody empiryczne, teoretyczne, techniki i narzędzia badawcze. W pracy został przedstawiony obszar i teren badań jak również została scharakteryzowana próba badawcza. Został także sformułowany główny problem badawczy, który brzmi następująco:, *Jakie zmiany należy wprowadzić w bezpieczeństwie systemu informacyjnego w uczelni wyższej, aby poprawić skuteczność ochrony informacji?*. Do przyjętego celu dysertacji i problemów badawczych na podstawie stanu posiadanej wiedzy jak i zgłębionej analizy literatury sformułowano główną hipotezę: *Założono, że obecny system informacyjny w organizacji publicznej na przykładzie uczelni wyższej nie w pełni chroni informację.*

Drugi rozdział pt. *Bezpieczeństwo systemu informacyjnego* z uwzględnieniem kontekstu teoretycznego i prawnego został poświęcony bezpieczeństwu systemu informacyjnego. Zostało omówione znaczenie informacji, systemów bezpieczeństwa informacyjnego w zakresie organizacji i państwa. W aspekcie prawnym zostały przybliżone obowiązujące akty normatywne z obowiązującymi regułami i normami. Przedstawiona została także diagnoza systemu informacyjnego funkcjonującego w uczelni wyższej.

Trzeci rozdział mający tytuł *Zagrożenia bezpieczeństwa systemu informacyjnego* poświęcony został zagrożeniom bezpieczeństwa systemu informacyjnego. Omówiona została strategia i aspekty systemu bezpieczeństwa. Ukazane zostały standardy i normy bezpieczeństwa systemu informacyjnego, obowiązujące w uczelni wyższej. Dokonana została charakterystyka występujących w uczelni wyższej zagrożeń bezpieczeństwa systemu informacyjnego wynikających z mnogości użytkowników i specyfiki jej funkcjonowania.

W rozdziale czwartym pt. *Koncepcja bezpieczeństwa systemu informacyjnego* została opracowana koncepcja bezpieczeństwa systemu informacyjnego odnosząca się do nowych propozycji zmian. Jej celem będzie poprawa bezpieczeństwa systemu informacyjnego na przykładzie uczelni wyższej. Ujęte zmiany dotyczą zasad funkcjonowania organizacji, bezpieczeństwa systemu informacyjnego w uczelni wyższej.

Każdy z rozdziałów posiada wnioski, będące wynikiem weryfikacji przyjętych hipotez i problemu badawczego. Dysertację wieńczą załączniki, czyli kwestionariusze ankiet dla grupy nauczyciele akademiccy, grupy kadra administracyjna i grupy studenci (różne kierunki). Dokonana została prezentacja zebranego materiału empirycznego pod

względem ilościowym i procentowym. Załączniki zawierają kwestionariusz wraz ze sprawozdaniem z badań ekspertów i arkusz bezpośredniej obserwacji. Dysertacja w wystarczający sposób wyczerpuje zagadnienie dotyczące bezpieczeństwa systemu informacyjnego w uczelni wyższej, które jest poparte analizą literatury, materiału empirycznego i przypadku.

Słowa kluczowe: system informacyjny, przekaz informacji, pracownicy, studenci, uczelnia wyższa, zagrożenia bezpieczeństwa systemu informacyjnego.

SUMMARY

This Dissertation entitled *Security of the Information System of a Public Organization on the example of a higher education institution* was aimed at evaluating the information system operating in a higher education institution. Nowadays, the society is being directed to transformations related to the use of digital technologies. The security of the information system was verified, taking into account the specifics of an organization such as a public university. The research was carried out on the internal user environment, which is characterized by a diverse structure aimed at the activities of the unit related to students' education, staff employment and scientific activities.

The main motive for writing the dissertation was the lack of an evaluation of the security of the information system in a higher education institution, which would comprehensively indicate the sources of threats and outline the directions, ways to implement changes in the studied area. Because of the new cognitive horizons resulting from the author's reflections using the literature on the subject and empirical material, and because of the attempt to show the concept of change in the area of information system security, the dissertation fits into the security sciences.

The dissertation extensively discusses threats to the security of the information system, which are currently not fully recognized, as well as the extent of their harmful effects cannot be predicted. In the academic community, as well as among the general public, there is a low awareness of the nature of information system security threats. The opportunity to get to know the academic community from the inside allowed the author to define the problem areas that contributed to the assessment of the level of information

system security at the university. The structure of the dissertation includes two parts namely, the theoretical part and the empirical part.

The dissertation consists of an introduction, four chapters, a conclusion, a bibliography, an index of figures, an index of tables, and appendices such as, a survey questionnaire, an expert interview questionnaire with a report, and an observation sheet. In order to verify the stated hypotheses, Pearson's linear correlation coefficient and coefficient of determination were calculated in the second, third, fourth chapters.

In the first chapter, titled *Methodology of own research*, issues relating to the object and purpose of the research were addressed. The research problem, working hypotheses and specific hypotheses are indicated. Empirical and theoretical methods, techniques and research tools are discussed. The paper presents the area and field of study, as well as characterizes the research sample. The main research problem was also formulated, which states:, *What changes should be made in the security of the information system in a higher education institution to improve the effectiveness of information protection?* To the adopted dissertation objective and research problems on the basis of the state of existing knowledge as well as the studied literature analysis, the main hypothesis was formulated: *It was assumed that the current information system in a public organization on the example of a higher education institution does not fully protect information.*

The second chapter entitled *Information system security* with theoretical and legal context was devoted to information system security. The signification of information, information security systems in terms of organizations and the state was discussed. In the legal aspect, on the other hand, the applicable normative acts with the applicable rules and standards were introduced. A diagnosis of the information system functioning in the university was also presented.

The third chapter, titled *Threats to the Security of the Information System*, is devoted to threats to the security of the information system. The strategy and aspects of the security system were discussed. The standards and norms of information system security in force in the higher education institution were presented. A characteristics of information system security threats occurring in a higher education institution, resulting from the multiplicity of users and the specifics of its operation, was made.

In the fourth chapter, entitled *Concept of information system security*, a concept of information system security directed at new directions of change was developed. Its purpose will be to improve the security of the information system on the example of

a higher education institution. The changes covered are related to the principles of organizational functioning, the security of the information system of a higher education institution.

Each chapter has a conclusion, which is the result of verification of the adopted hypotheses and the research problem. The dissertation is ended with appendices, i.e. survey questionnaires for the group of academic teachers, the group of administrative staff and the group of students (various majors). This is a presentation of the collected empirical material in terms of quantitative and percentages. The appendices include a questionnaire with an expert research report and a direct observation sheet. The dissertation sufficiently exhausts the issue of information system security in a higher education institution, which is supported by the analysis of literature, empirical material and the case.

Keywords: information system, information transfer, employees, students, university, information system security threats.

WSTĘP

Środowiska wyposażone w narzędzia gromadzące technologię informatyczną, informacyjną w systemach komunikacyjnych przyczyniły się do wykreowania społeczeństwa informacyjnego. Owo społeczeństwo charakteryzuje łatwość użytkowania wszelkiego typu systemów informatycznych i technologii cyfrowych, komputerów, Internetu oraz telefonów komórkowych do przesyłania jak i do zdalnego przetwarzania informacji. Dzięki takim rozwiązaniom jest zauważalny wśród członków społeczeństwa rozwój społeczny, osobisty, zawodowy i kulturowy. Nie wszyscy użytkownicy Internetu, komputerów, telefonów posiadają umiejętności ich obsługi w związku z powyższym taka sytuacja nakierowuje do działań przestępczych. Wszelkie działania wykorzystywane przez hakerów najczęściej polegające na pozyskaniu haseł do kont użytkowników, przesyłanie zawirusowanych linków, Trojanów itp..

Działania hakerskie w obecnych czasach są bardzo trudne do wykrycia, zaś rozmiar ich szkodliwości dla pozyskanych, przechowywanych danych, systemów informacyjnych, sprzętu teleinformatycznego często wśród osób potencjalnie zagrożonych przerasta ich wyobraźnię. Problem nieświadomości społeczeństwa informacyjnego i nieodpowiedzialnego korzystania z sieci jak również z narzędzi teleinformatycznych, obliguje do wywołania dyscyplinujących zmian w postawach użytkowników a w dalszej perspektywie prowadzi do zwiększenia bezpieczeństwa w cyberprzestrzeni. W związku z faktem, iż często użytkownicy sieci pomijają zabezpieczenia systemowe a wówczas powstają zjawiska związane z cyberprzestępczością.

Znaczenie strategiczne ma wpływ na informację w sferze obronności państwa, technologicznej, ekonomicznej, społeczno-kulturowej, polityczno-prawnej. Informacja jest wykorzystywana w komunikacji, kształtuje procesy decyzyjne oraz stymuluje zachowania w środowisku społecznym. Stała się ona obiektem zainteresowania m.in. dla środowisk przestępczych. Poczucie anonimowości oraz mnogość informacji znajdującej się w sieci jest potencjalnym zagrożeniem dla środowiska informacyjnego będącego jej odbiorcą.

Na uczelni wyższej, jako organizacji publicznej, zapewnienie bezpieczeństwa systemu informacyjnego jest wysoce cenione i we współczesnej rzeczywistości rynkowej stanowi o jej umocnieniu i sile. Uczelnią wyższą kieruje rektor, a do jego podstawowych zadań należy m.in. reprezentowanie, zarządzanie uczelnią, zapewnienie wykonywania

przepisów obowiązujących w uczelni. Na rektorze spoczywa odpowiedzialność za organizację oraz zasady działania spraw administracyjnych w jednostkach organizacyjnych.

Uczelnie wyższe i ich działanie powinny opierać się na utrzymaniu wysokich standardów bezpieczeństwa informacyjnego, mające przełożenie na bezpieczeństwo całego kraju. Rektor w kierowaniu uczelnią wyższą powinien się kierować polityką bezpieczeństwa informacyjnego wśród kadry naukowo-dydaktycznej, dydaktycznej, naukowej, administracyjnej oraz wśród studentów realizujących kształcenie w poszczególnej jednostce znajdującej się w uczelni. Swoje decyzje powinien opierać na planowaniu, inspirowaniu i zajmowaniu się zagadnieniami kluczowymi w skali organizacji.

Kluczowym jest fakt, iż jest on zaangażowany w problematykę dotyczącą rozwoju teorii zarówno w zakresie nauki organizacji i zarządzania jak również dyscyplinie podstawowej dla profilu działalności organizacji[1]. Rezolutność i rzeczowość w zarządzaniu informacją pokazuje wysokie kompetencje menedżerskie rektora i chęć podążania uczelni wyższej w kierunku nieustannego rozwoju tak potrzebnego w czasach ówczesnych, aby dorównać zmienności potrzeb.

Do zwiększenia uwagi na problem związany z bezpieczeństwem danych osobowych w jednostkach organizacyjnych przyczyniły się takie prawne aspekty jak, Konstytucja RP, Rozporządzenia Parlamentu Europejskiego i Rady UE 2016/679 (tzw. RODO) z dnia 27 kwietnia 2016 r. jak i Ustawa o ochronie danych osobowych z dnia 10 maja 2018 r..

W rozprawie doktorskiej został objęty analizą poziom bezpieczeństwa systemu informacyjnego w uczelni wyższej. Zakres podmiotowy skupia się na organizacji publicznej, czyli uczelni wyższej. Publiczna uczelnia wyższa jest organem, który jest miejscem pracy dla wszystkich osób w niej zatrudnionych. Realizuje ona również zadania oświatowe, kształci z jednoczesnym wychowaniem i sprawowaniem opieki nad studentami z uwzględnieniem profilaktyki społecznej. Przeznaczenie uczelni wyższej do celów edukacyjnych społeczeństwa w myśl ustawy o szkolnictwie wyższym i nauce, wymaga pozyskania wykwalifikowanej kadry pracowników zarówno naukowo-badawczych, dydaktycznych, naukowych jak i kadry administracyjnej zajmującej się przetwarzaniem informacji oraz obiegiem dokumentacji.

Jakże ważnym elementem jest odpowiednia infrastruktura będąca w posiadaniu jednostki. Szczególnym wyzwaniem dla rektora jest zarządzanie tak dużą ilością osób

[1] J. Wołejszo, *Organizacja pracy kierownika w organizacji zhierarchizowanej,* „Zeszyty Naukowe AON", nr 2(91), 2013, s. 27.

w podległej mu organizacji publicznej a co za tym idzie utrzymanie pełnego bezpieczeństwa systemu informacyjnego. W związku z tak szybko postępującym procesem informacyjnym należy wnikliwiej spoglądnąć i przeanalizować poziom bezpieczeństwa systemu informacyjnego w uczelniach wyższych. Koniecznym jest fakt, aby wzmacniać kanały przekazywania informacji, które nie są w należyty sposób chronione, kontrolowane przed dostępem osób trzecich. Przydział zakresów obowiązków, dodatkowych zadań, uprawnień w znaczącym stopniu rektorowi utrudnia precyzyjną ocenę zakresu zapewnienia bezpieczeństwa systemu informacyjnego.

Każda organizacja tak jak i uczelnia wyższa podejmuje decyzje w obszarach procesu zarządzania, którymi są planowanie wraz z podejmowaniem decyzji, organizowanie, motywowanie, kontrolowanie. Powyżej wskazane działania dotyczą również sfery bezpieczeństwa systemu informacyjnego. Możliwość zdefiniowania obszaru problemowego, który przyczynił się w dużej mierze do oceny bezpieczeństwa systemów informacyjnych w uczelni wyższej. Autorka miała możliwość to środowisko poznać i ocenić od wewnątrz.

Struktura rozprawy doktorskiej obejmuje dwie części, jedną teoretyczną, drugą empiryczną. Dysertacja zawiera wstęp, cztery rozdziały, bibliografię, spis tabel, rysunków, wykresów, jak i załączników.

Rozdział pierwszy mający tytuł *„Metodologia badań własnych”,* został poświęcony metodologii, przedmiotu oraz celu badań. Został zaprezentowany główny problem badawczy, hipotezy szczegółowe i robocze. Zostały także omówione metody, techniki, narzędzia badawcze oraz dokonano przedstawienia obszaru i terenu badań. Wskazana została także charakterystyka próby badawczej.

W rozdziale drugim mającym tytuł *„Bezpieczeństwo systemu informacyjnego”* zostały poruszone kwestie bezpieczeństwa systemu informacyjnego, jego kontekst prawny. Zostały poruszone obowiązujące akty normatywne wraz z regulacjami, normami powszechnie obowiązującymi. Omówieniu zostało poddane znaczenie systemów bezpieczeństwa informacyjnego dla państwa, jako szerszej struktury oraz organizacji w jej węższym znaczeniu. W tym rozdziale została przedstawiona diagnoza systemu informacyjnego funkcjonującego w uczelni wyższej.

Rozdział trzeci mający tytuł „*Zagrożenia bezpieczeństwa systemu informacyjnego”* zostały w nim wyszczególnione zagrożenia bezpieczeństwa systemu informacyjnego wraz z omówieniem aspektu systemu bezpieczeństwa i jego strategii. Dokonana została charakterystyka ograniczeń i zagrożeń bezpieczeństwa systemu informacyjnego.

Zostały również przedstawione normy i standardy, jakie są wprowadzone i obowiązują w uczelni wyższej.

W rozdziale czwartym mającym tytuł *„ Koncepcja bezpieczeństwa systemu informacyjnego”* została opracowana koncepcja poruszonego w pracy doktorskiej bezpieczeństwa systemu informacyjnego, której zadanie polega na ukazaniu nowych kierunków zmian mających na celu poprawę bezpieczeństwa systemu informacyjnego na przykładzie uczelni wyższej. Zmiany te dotyczą zasad funkcjonowania oraz organizacji bezpieczeństwa systemu informacyjnego w uczelni wyższej.

Każdy z rozdziałów został zakończony wnioskami będącymi wynikiem weryfikacji hipotez przyjętych przez autorkę oraz wnioskiem końcowym wynikającym z omawianego problemu badawczego.

Dysertację wieńczą przygotowane załączniki, czyli kwestionariusze ankiet dla trzech grup badawczych tj. nauczycieli akademickich, kadry administracyjnej, studentów (różnych roczników). Dokonana została prezentacja pozyskanego materiału empirycznego pod względem procentowym, ilościowym, uwzględniając jakże ważny wskaźnik struktury. W pozostałych załącznikach znajduje się arkusz obserwacji bezpośredniej, organizacji i funkcjonowania publicznej uczelni wyższej oraz sprawozdanie z badań opinii ekspertów.

METODOLOGIA BADAŃ WŁASNYCH

1.1.Uzasadnienie wyboru tematu

Informacje, jako aktywa każdego podmiotu narażone są na liczne zagrożenia istniejące w otaczającym nas świecie a w szczególności w cyberprzestrzeni. Zarządzanie informacją może być niedoskonałe jak również nieudolne, skutkując poważne konsekwencje wywołujące naruszenie stabilizacji organizacji a w najgorszym przypadku może doprowadzić do destrukcji.

Podjęcie się badaniu poziomu bezpieczeństwa systemu informacyjnego w uczelni wyższej w ramach rozprawy doktorskiej pozwoliło na faktyczną ocenę jego rzeczywistego stanu. Biorąc pod uwagę środowisko uczelniane badanej organizacji publicznej, a pozyskane wyniki mają przełożenie na ogólną ocenę bezpieczeństwa informacyjnego w uczelni wyższej i tym samym bezpieczeństwa narodowego. Posiadanie pełnej wiedzy uświadomiło potrzebę konieczności zwiększenia działań prewencyjnych we wspomnianym zakresie. Polityka bezpieczeństwa zwyczajowo powinna być formowana przez rektora uczelni wyższej przy jednoczesnym wsparciu osób, którym zostały powierzone zadania związane z ochroną informacji znajdujących się w gestii wspomnianego podmiotu.

Badania dowiodły, iż nie w pełnym zakresie są one chronione[1]. W związku z powyższym cel pracy skupił się na znalezieniu skutecznych rozwiązań, których zastosowanie pozwala wpłynąć z jednej strony na zwiększenie bezpieczeństwa systemu informacyjnego w organizacji publicznej, jaką jest uczelnia wyższa a z drugiej strony na poprawie, jakości informacji. Wykonana praca miała charakter poznawczy a jej skutkiem było wnikliwe zbadanie i poszerzenie wiedzy na temat systemu obiegu informacji w publicznej organizacji, jaką jest uczelnia wyższa.

Badania nad informacją są w trakcie rozwoju, ponieważ komunikacja jest tematem zainteresowania filozofii, teorii literatury czy chociażby antropologii kulturowej. Fakt ten pokazuje, że informacja staje się powszechnym, uniwersalnym tematem komunikacji a pośrednio nawet i powszechnej wiedzy. Czynna rola informacji i jej istota w życiu społecznym i poszczególnych jednostek ujawnia się w momencie jej funkcjonowania w różnych układach komunikacyjnych[2]. Poszukiwanie skutecznych systemów chroniących informację przed zagrożeniami płynącymi z zewnątrz i wewnątrz organizacji ma

[1] K. Liderman, *Bezpieczeństwo informacyjne. Nowe wyzwania,* PWN, Warszawa 2017, s. 129.
[2] M. Hetmański, *Świat informacji,* Difin, Warszawa 2015, s. 142.

ogromne znaczenie w rozwoju współczesnych technik na świecie a co za tym idzie pokolenia informacyjnego.

Doświadczenie wynikające z pracy w organizacji publicznej w tym przypadku uczelni wyższej ma kluczowe znaczenie w oglądzie wewnętrznego jej funkcjonowania, panujących zasadach oraz dystrybucji informacji w trzech wymiarach, fonetycznym, tekstowym i graficznym, co jednoznacznie wskazuje na możliwość wystąpień zagrożeń systemów informacyjnych. Właściwe zarządzanie uczelnią wyższą, skuteczne niwelowanie ryzyka związanego z powszechnym obiegiem informacji może tylko zagwarantować ustawiczna kontrola stanu bezpieczeństwa systemu informacyjnego.

Uwarunkowania wygenerowały sytuację problemową w związku z powyższym zaszła potrzeba ustalenie stanu faktycznego wpływu uczelni wyższej na system obiegu informacji mającym jednoczesne uwzględnienie w relacji wewnętrznej jak i określenia, jakich organizacyjnych zmian należy dokonać, aby usprawnić skutecznie realizację zadań przy jak najefektywniejszym wykorzystaniu posiadanej informacji.

Powody wyboru tematyki dysertacji:

- potrzeba określenia zasad wykorzystania informacji pomiędzy stanowiskami wewnątrz uczelni wyższej;
- potrzeba zwiększenia kontroli przepływu informacji przez wszystkich uczestników systemu informacyjnego w uczelni wyższej;
- niska świadomość istoty piętrzącego się potencjalnego zagrożenia bezpieczeństwa systemu informacyjnego w uczelni wyższej jak i wśród społeczeństwa;
- autorka będąca pracownikiem wchodzącym w skład kadry administracyjnej na uczelni wyższej, podejmuje wiele zadań, subiektywnie dokonała oceny, że istnieje potrzeba zmodyfikowania, ulepszenia aktualnego systemu bezpieczeństwa informacyjnego w celu zapewnienia skutecznej realizacji zadań wynikających z potrzeby działań w organizacji jaką jest uczelnia wyższa.

1.2. Przedmiot badań i cele badawcze

Przedmiotem badań jest ***system bezpieczeństwa informacyjnego w organizacji publicznej na przykładzie uczelni wyższej.***

Sytuacja problemowa przyczyniła się do powstania celu badań mających następujące brzmienie:

Cel poznawczy*:* określenie poziomu bezpieczeństwa systemu informacyjnego organizacji publicznej na przykładzie uczelni wyższej.
Cel praktyczny: opracowanie koncepcji bezpieczeństwa systemu informacyjnego w uczelni wyższej.

1.3. Problem badawczy

Główny problem badawczy w odniesieniu do przyjętego celu został sformułowany w postaci pytania:, ***Jakie zmiany należy wprowadzić w bezpieczeństwie systemu informacyjnego w uczelni wyższej, aby poprawić skuteczność ochrony informacji?***

Żeby uzyskać odpowiedź na powyżej wskazany główny problem badawczy należy pozyskać szereg odpowiedzi na proponowane problemy szczegółowe, które brzmią następująco:
1. Jakie uwarunkowania wpływają na bezpieczeństwo systemu informacyjnego w uczelni wyższej?
2. Jakie występują zagrożenia bezpieczeństwa systemu informacyjnego w uczelni wyższej?
3. Jaka powinna być koncepcja bezpieczeństwa systemu informacyjnego w uczelni wyższej?

1.4. Hipotezy robocze

Na podstawie przyjętego celu i problemów badawczych wynikających ze stanu posiadanej wiedzy, przeanalizowanej literatury jak i prognozowanych zmian została sformułowana wstępna hipoteza nosząca brzmienie: ***Założono, że obecny system informacyjny w organizacji publicznej na przykładzie uczelni wyższej nie w pełni chroni informację.*** Do tak sformułowanej wstępnej hipotezy głównej przyjęto następujące hipotezy szczegółowe:

(H1) Założono, iż bezpieczeństwo systemu informacji w uczelni wyższej znajduje swoje uregulowanie pośrednio i bezpośrednio w źródłach powszechnie obowiązującego prawa. Do takich źródeł należy zaliczyć m.in. Konstytucję RP, ratyfikowane umowy międzynarodowe, ustawy, rozporządzenia oraz akta prawa miejscowego, które swoim zasięgiem obejmują obszar działania organów, które je ustanowiły. Bezpieczeństwo systemu

informacyjnego w ogromnym stopniu przekłada się na współpracę pomiędzy jednostkami i fakt ten świadczy o wysokim standardzie zarządzania jednostką organizacyjną. Bez informacji i jej właściwego procedowania w systemie nie ma możliwości, aby nastąpiło efektywne, poprawne i szybkie wykorzystanie działalności analitycznej pozwalającej na zwiększenie bezpieczeństwa państwa oraz jego obywateli[1].

(H2) Założono, że dochodzi do wystąpienia zagrożenia w bezpieczeństwie systemu informacyjnego w uczelni wyższej. Powodem mogą być luki w dotychczasowych zabezpieczeniach informacji a wymagane procedury w celu zapewnienia bezpieczeństwa informacyjnego nie były przez wszystkich użytkowników w należyty i kompetentny sposób przestrzegane. Duża ilość użytkowników systemu informacyjnego zmniejsza poziom jego bezpieczeństwa poprzez wykorzystanie fragmentaryczne, wszystkich mających istotny wpływ zabezpieczeń i procedur. Wśród osób korzystających ze środków przekazu informacji pojawiał się brak świadomości czy chociażby odpowiedzialności o skutkach łamania zasad korzystania z systemu informacyjnego. Do typowych zagrożeń systemu bezpieczeństwa związanych z obiegiem informacji należy zaliczyć m.in. przestępstwa przy użyciu komputera, cyberterroryzm, utrata danych, informacji związana z przesyłaniem złośliwych zawirusowanych linków, kodów. Poważnymi zagrożeniami, o których nie należy zapomnieć to wandalizm, sabotaż, szpiegostwo.

Dzięki lokalizacji źródeł zagrożenia można wyodrębnić zagrożenia wewnętrzne systemu bezpieczeństwa informacyjnego, mające swoje korzenie wewnątrz organizacji i są to m.in. utrata, celowe uszkodzenie posiadanych danych przez osoby zewnętrzne oraz przypadkowe uszkodzenie z powodu błędu, pomyłki braku odpowiedniego przeszkolenia. Założono również ze można wyodrębnić zagrożenia fizyczne, których zaistniała szkoda jest podyktowana wypadkiem, awarią lub innymi zdarzeniami, nieprzewidzianymi mającymi wpływ na system informacyjny. Dla lepszego zobrazowania dokonano podziału tych zagrożeń na:

- *losowe,* katastrofy, klęski żywiołowe, wypadki, zagrożenia te mają wpływ na stan bezpieczeństwa informacyjnego organizacji w odniesieniu do powodzi, pożarów budynków, w których nośniki informacji są przechowywane;

[1] K. Liedel, P. Piasecka, T. R. Aleksandrowicz, *Analiza informacji. Teoria i praktyka zarządzanie bezpieczeństwem,* Difin, Warszawa 2012, s. 33.

- *tradycyjne zagrożenia informacyjne,* charakteryzujące się szpiegostwem, sabotażem oraz ofensywa dezinformacyjna kontrolowana przez obce podmioty, organizacje czy też państwa;
- *technologiczne,* tego typu zagrożenia związane są z gromadzeniem, przetwarzaniem

i przekazywaniem danych (informacji) w sieciach teleinformatycznych. Należy tutaj wyszczególnić przestępstwa komputerowe, walkę informacyjną, cyberterroryzm;

- *odnoszące się do praw obywatelskich,* sprzedaż pozyskanych informacji, przekazywanie informacji nieupoważnionym podmiotom, bezprawne ingerencje służb specjalnych, ograniczenie jawności życia publicznego oraz naruszenie prywatności.

Założono, że decydującymi elementami dotyczącymi bezpieczeństwa obiegu informacji były zarówno braki dostatecznej wiedzy pracowników biorących udział w procesie obiegu informacji jak i elementy mające podłoże kryminogenne. W następstwie postępu gospodarczego, bezpieczeństwo obiegu informacji mogą zachwiać takie elementy jak, ludzka ciekawość, korupcja. Przy ciągle rosnącej w obecnych czasach liczbie przestępstw dochodzi do rozwoju także działalności wywiadu gospodarczego.

(H3) Założono, iż należy opracować koncepcję bezpieczeństwa systemu informacyjnego w uczelni wyższej, aby nastąpiło zwiększenie skuteczności jak również efektywności zabezpieczeń informacji. Założenia autorki dotyczyły implementacji zmian w zasadach funkcjonowania, użytkowania i organizacji systemu informacyjnego w uczelni wyższej.

Kluczowa była potrzeba skonkretyzowania kompetencji użytkowników, ich jakże szerokie poczucie odpowiedzialności za utrzymanie stanu bezpieczeństwa informacyjnego.

W obszarze organizacyjnym nastąpiła konieczność zastosowania integracji systemu informacyjnego wszelkich komórek organizacyjnych (działów) występujących w uczelni wyższej. Celem było osiągniecie efektu synergii działań. Nie można było pominąć w koncepcji bezpieczeństwa informacyjnego, istoty zapewnienia efektywnej płaszczyzny porozumienia jak i dobrych praktyk mieszczących się w zakresie współpracy poszczególnych ogniw operacyjnych występujących w uczelni wyższej.

Założono, że kontrola i nadzór w organizacji publicznej nad obiegiem informacji powinna mieć miano wystarczającej, systematycznej oraz skutecznej. Elementami decydującymi o ich skuteczności jest, częstotliwość, dokładność przeprowadzenia, a systematyczny nadzór wielopłaszczyznowy zwiększa bezpieczeństwo informacji będących w obiegu.

Przy opracowaniu koncepcji dotyczącej bezpieczeństwa systemu informacyjnego w uczelni wyższej został uwzględniony fakt, że wspomniane wyżej bezpieczeństwo informacyjne w żadnym razie nie dotyczy wyłącznie samej informacji. Obejmujący zakres jest szerszy i dotyczy systemu, w którym jest ona wytwarzana, przetwarzana, przechowywana a nawet przekazywana dalej. Chodzi o środowisko, w którym ten system działa, jego użytkowników a także całego otoczenia formalno-prawnego, kształtującego zarówno procesy użytkowania informacji jak i technologie informacyjne. W owym przypadku system informacyjny zarządzania powinien być wprowadzony w uczelni wyższej ułatwiłoby to gromadzenie informacji niezbędnych do funkcjonowania procesu, usprawnienie, eliminację zbędnych pośrednich procesów, zmniejszenie czynnika ludzkiego w procesie jak również poprawiłoby skuteczność i bezpieczeństwo obiegu informacji.

1.5. Metody, techniki, narzędzia badawcze

W procesie badawczym zostały zastosowane metody badania poziomu bezpieczeństwa systemu informacyjnego w uczelni wyższej o podłożu empirycznym i teoretycznym.

- **empiryczne,** obserwacja, metoda sondażu diagnostycznego przy wykorzystaniu narzędzi badawczych tj. kwestionariusz ankiety i wywiadu,
- **teoretyczne,** analiza, synteza, abstrahowanie, uogólnienie, porównanie, wnioskowanie, wskazane metody badawcze zostały zastosowane podczas realizacji wszystkich etapów prowadzonych badań, zaś dobór wynikał z charakteru problemu badawczego.

Jedną z metod empirycznych była **obserwacja**, będąca procesem uważnego i celowego postrzegania. Jest ona także gromadzeniem, interpretowaniem pozyskanych, zgłębionych danych w ich naturalnym przebiegu, kiedy pozostają w bezpośrednim polu

słyszenia i widzenia dla obserwatora. W metodzie obserwacji można wyróżnić podstawowe etapy tj.: postrzeganie, gromadzenie, interpretowanie[1]. Wspomniane etapy nie następują po sobie według kolejności i nie są od siebie w żaden sposób zależne. Może zdarzyć się tak, że postrzeganie zjawisk przebiegnie jednocześnie z ich gromadzeniem czy interpretowaniem. Jednakże z naukowego punktu widzenia obserwacja obejmuje w pierwszej kolejności postrzeganie danych, następnie ich utrwalanie a już na samym końcu próbę ich interpretacji. Interpretacja mająca miano trafnej powoduje, że obserwacja nie jest bezprzedmiotowa z punktu widzenia nauk społecznych oraz jałowa[2]. Metoda obserwacji uczestniczącej pozwoliła autorce na wniknięcie w środowisko uczelniane z możliwością obserwacji badanej organizacji od wewnątrz. Początkowa faza badań skłoniła do refleksji nad sytuacją problemową, zaś w końcowym efekcie była wyjściem do podjęcia badań jak i sformułowania celu ich prowadzenia.

Kolejna zastosowana metodą empiryczna była to **metoda sondażu diagnostycznego**, jej przyjęcie wynikało z celu i przedmiotu badań. Wspomniana metoda jest sposobem gromadzenia wiedzy o atrybutach funkcjonalnych, strukturalnych, jak również dynamice zjawisk społecznych, poglądach, opiniach zawężonej zbiorowości, kierunkach rozwoju, nasileniu się określonych zjawisk jak i wszelkiego rodzaju innych zjawisk niezlokalizowanych instytucjonalnie (posiadających znaczenie wychowawcze w oparciu o specjalnie dobraną grupę mającą reprezentować populację generalną w obrębie, której to badane zjawisko występuje)[3]. Metoda ta miała duży wpływ na rozwiązanie większości szczegółowych problemów badawczych a ich wyniki zostały przedstawione w poniższych rozdziałach.

Metody teoretyczne pozwoliły uzyskać materiał badawczy zawarty w bibliografii, wyodrębniając składniki istotne w procesie badawczym. W następnej kolejności umożliwiły porównanie i syntezę wyodrębnionych składowych elementów w celu uzyskania niezbędnego materiału do dalszych badań.

Jedną z metod badawczych była **analiza**, oparta na zdolności umysłu ludzkiego do myślowego rozdzielenia rzeczy, zjawisk, zdarzeń jak i złożonych procesów, aby je lepiej poznać. Analiza była podstawą sprecyzowania problemów badawczych, pozwoliła

[1] *Participant Obseryation and the CoUecfion and Interpretation of Data,* „American Journal of Sociology", t. 40, 1955, s. 355.
[2] C. Frankfort-Nachmias, D. Nachmias, *Metody badawcze w naukach społecznych,* Wydawnictwo Zysk i S-ka, Poznań 2001, s. 223.
[3] T. Pilch, T. Barman, *Zasady badań pedagogicznych. Strategie jakościowe i ilościowe*, Żak Wydawnictwo Akademickie, Warszawa 2018, s. 80

na przedstawienie i uzasadnienie ważności sprecyzowanych problemów i sformułowania hipotez roboczych. W procesie badawczym analiza występuje i wiąże się wzajemnie z syntezą.

W pewnym stopniu analiza warunkuje syntezę a synteza może stanowić punkt wyjścia do kolejnych analiz. Procedury analityczne precyzują problem naukowy i wysuwane są hipotezy, mające postać syntetyczną. Oczywistym jest fakt, iż w poszczególnych konkretnych badaniach, pracach naukowych, treści danego myślenia, wytworzonej wiedzy naukowej może dominować albo analiza albo synteza[1]. Powyższa metoda badawcza została wykorzystana we wszystkich rozdziałach pracy z zastosowaniem techniki analizy ilościowej i jakościowej. Ta metoda została zastosowana również w trakcie analizowania literatury i objęła gromadzenie, selekcję informacji zawartych w literaturze, dokumentach normatywnych nakierowanych na bezpieczeństwo systemu informacyjnego. Pozwoliło to na zgłębienie wiedzy w obszarze problematyki badawczej.

Kolejną z metod badawczych była **synteza** opierająca się na zdolności umysłu ludzkiego do łączenia myślowego według określonej zasady zjawisk, rzeczy, zdarzeń itd. uprzednio rozdzielonych w celu ich lepszego poznania. Synteza powinna nadawać nową lepszą, jakość. Jak również ma umożliwić poznanie istoty i w jak najskuteczniejszy sposób wykazać najważniejsze właściwości badanego obiektu, zjawiska czy nawet procesu. Synteza nie jest odwróceniem analizy, gdyby jednak rzeczywiście była to nie pełniłaby roli samoistnej, a jedynie role sprawdzającą w stosunku do analizy. Istota syntezy polega na tym, ze dochodzi ona przez długie i splątane drogi rozważań do nowych, całkiem nieoczekiwanych wyników[2]. Powyższa metoda została wykorzystana we wszystkich poniższych rozdziałach.

Następną użytą metodą badawczą było **abstrahowanie** a wykorzystana została do czynności tj.: pomijania, czyli eliminowania, odłączania, czyli izolacji oraz wyodrębniania. Wymienione czynności mogą stanowić istotę abstrakcji polegającej na wyłonieniu pewnych elementów badań przedmiotu, pod pewnym względem uznanych za nieistotne lub drugorzędne. Badacz w ramach tej metody w swoich rozważaniach powinien uwzględnić inne elementy, będące pod pewnymi względami nieistotne[3].

[1] E. Wiśniewski, *Metodyka wojskowych badań naukowych*, „Zeszyty Naukowe ASG WP" cz. 1(3), 1990, s. 61.
[2] W. Pytkowski, *Organizacja badań i ocena prac naukowych*, PWN, Warszawa 1985, s. 114.
[3] Tamże, s. 74.

Uogólnienie zastosowane zostało, jako element podsumowujący każdą kolejną fazę pracy badawczej, pojawiło się w rozdziale końcowym pracy, łącząc wyniki badań jakościowych i ilościowych. Wspomniane uogólnienie to podobieństwo zjawisk, występujących w nich wspólnych cech, pozwala na formułowanie ogólniejszych twierdzeń. Metoda ta jest operacją myślową przechodzenia od twierdzeń o pojedynczym zjawisku do twierdzeń bardziej ogólnych dotyczących klasy zjawisk, grup a w dalszej części do jeszcze bardziej ogólnych itd.. Tworzy się to za pomocą łączenia faktów na zasadzie stwierdzenia ich podobieństw pod jakimś konkretnym kątem[1].

Porównanie to metoda badawcza polegająca na zestawieniu pewnych cech wspólnych, różniących dany przedmiot badań lub zjawisko. W pracy zostały zastosowana synteza na wszystkich etapach prac badawczych, istotą, których była identyfikacja wspólnych cech, podobieństw czy różnic poszczególnych zagadnień badawczych przede wszystkim w zakresie obiegu informacji w publicznej organizacji i bezpieczeństwa tego procesu. Porównanie to zostało przeprowadzone w sytuacji zestawienia skonstruowanego systemu obiegu informacji z obecnie funkcjonującym systemem obiegu informacji działającym w uczelni wyższej.

Spoistym elementem prowadzonego procesu badawczego była **metoda wnioskowania**, czyli rozumowania. Wnioskowanie zastosowane zostało we wszystkich rozdziałach w części, w której znalazły się wnioski jak i w zakończeniu dysertacji. Wnioskowanie subiektywne pewne zostało przeprowadzone wedle schematu niezawodnego a mianowicie[2]:

Każde X jest Y
Każde Z jest X
Każde Z jest Y

Do metody wnioskowania, pozwalającej badaczom określić charakter badanych cech czy zdarzeń, tworząc jednolity proces badawczy zaliczyć należy **dedukcję i redukcję**.

[1] E. Wiśniewski, *Metodyka wojskowych …dz. cyt.*, s. 79.
[2] K. Ajdukiewicz, *Logika pragmatyczna*, PWN, Warszawa 1965, s. 109.

Dedukcja to rozumowanie polegające na odtwarzaniu faktów (implicite oraz explicite) zawartych we wniosku ogólnym[1]. Oparte jest o wnioskowanie formalne poprawne, innymi słowy realizowane poprzez dany schemat logiczny, np. transpozycję[2]. Zastosowanie dedukcji miało miejsce przy wskazaniu czynników, mogących wpłynąć na bezpieczeństwo systemu informacyjnego w uczelni wyższej.

Redukcja i wnioskowanie na podstawie teoretycznej metody badawczej pojawia się w sytuacji, kiedy z *przesłanek tego wnioskowania nie wynika jego wniosek, natomiast z wniosku tego wnioskowania wynikają przesłanki*[3]. Wspomniana redukcja może być traktowana, jako powrót do następstw przyczyn pod warunkiem, że jest to typ wnioskowania zawodowego[4]. Zastosowanie redukcji w badaniu odbyło się podczas wskazania i opisania rezultatów stosowania systemu obiegu informacji w uczelni wyższej.

W dysertacji zostały wykorzystane elementy statystyki[5], posłużyły one do ustalenia związków sądów jak i opinii z przynależnością do syntezy myślowej cząstkowych opinii i sądów uzyskanych w trakcie ankietowego badania mając na celu uogólnienie pozyskanych wnyków oraz do wyodrębnionych grup respondentów. W ramach pogrupowania zebranego materiału empirycznego zostały utworzone szeregi statystyczne, dokonano analizy korelacji i estymacji pomiędzy zmiennymi i zastosowano graficzną prezentację danych, do której wykorzystano arkusz kalkulacyjny Microsoft Excel.

W związku z koniecznością sprawdzenia postawionych hipotez został obliczony **współczynnik korelacji liniowej Persona** jak również **współczynnik determinacji**. Opierając się o analizę pozyskanych wyników została określona korelacja pomiędzy poszczególnymi zmiennymi, zmiennej niezależnej x_i i zmiennej zależnej $y_{i,}$ i odpowiedź czy udzielone odpowiedzi mają związek z przynależnością respondentów do poszczególnych grup badawczych. W związku z faktem, że badania zostały przeprowadzone na próbie statystycznej, obliczony współczynnik współzależności cech upoważniał do formułowania tylko i wyłącznie wniosków najbardziej prawdopodobnych mających określoną siłę korelacji miedzy zmiennymi.

---

[1] M. Łobocki, *Wprowadzenie do metodologii badań pedagogicznych*, Oficyna Wydawnicza Impuls, Kraków 2001, s. 50.
[2]K. . Ajdukiewicz, *Zarys logiki*, PZWS, Warszawa 1956, s. 162.; K. Ajdukiewicz, Logika…, op. cit. s. 160-161.
[3] K. Ajdukiewicz, *Zarys…dz. cyt. ,*s. 127-133.
[4] M. Pelc, *Wybrane problemy metodologiczne wojskowych badań naukowych, AON,* Warszawa 1998, s. 18-19.; M. Pelc, *Elementy metodologiczne badań naukowych.,* AON, Warszawa 2012, s. 24.
[5] Statystyka to nauka zajmująca się metodami badania przedmiotów i zjawisk w ich masowych przejawach oraz ich ilościową lub jakościową analizą z punktu widzenia dyscypliny naukowej, w której zakres wchodzą. Zob. M. Kędelski, I. Roeske-Słomka, *Statystyka*, AE Poznań, Poznań 1998, s. 10.

Współczynnik wcześniej wspomnianej korelacji liniowej Persona, został oznaczony symbolem r_{xy}, jest on miernikiem siły związku prostolinijnego pomiędzy dwiema cechami mierzalnymi. Owym związkiem nazywana jest zależność, w której przyrostem jednostkowym jednej zmiennej towarzyszy średnio stały przyrost zmiennej drugiej, (mowa tu o przyczynie i skutku) oraz wskazującego kierunek korelacji wraz z jego natężeniem[1]. Następujący wzór wyznacza współczynnik korelacji liniowej Persona, w którym $S_{(x)}$ i $S_{(y)}$ mają miano odchyleń standardowych odpowiednich zmiennych[2].

$$r_{xy} = \frac{\frac{1}{n}\sum_{i=1}^{n}(x_i-\overline{x})(y_i-\overline{y})}{S_{(x)}S_{(y)}}$$

gdzie:

n-oznacza liczbę obserwacji

$\overline{x}$ y - oznacza wartości badanych zmiennych,

$S_{(x)}$ – oznacza odchylenie standardowe zmiennej x_i

$S_{(y)}$ – oznacza odchylenie standardowe zmiennej y_i

W odniesieniu do kierunku i siły zależności między ustalonymi grupami respondentów i wyrażonych przez nich opinii wykorzystano poniższe zależności wraz ze skalą zmienności. Najważniejsze właściwości współczynnika korelacji liniowej Pearsona r_{xy} są przedstawione następująco:

- współczynnik korelacji Pearsona może przyjmować wartości z przedziału <-1;1>;
- $r_{xy}=0$ – jeżeli cechy są liniowo nieskorelowane i im jest bliższy „0”, tym związek jest słabszy;
- $|r_{xy}| =1$, jeżeli występuje zależność funkcyjna , znak współczynnika korelacji wskazuje kierunek zależności:
  + dodatnia korelacja, - ujemna korelacja[3].

Przyjęte zostały następujące przedziały do oceny siły współzależności:

- |0,0-0,2| - współzależność bardzo słaba;
- |0,2-0,4| - współzależność słaba;
- |0,4-0,6| - współzależność umiarkowana;
- |0,6-0,8|- współzależność silna;

[1] M. Sobczyk, *Statystyka*, PWN, Warszawa 2007, s. 237.
[2] M. Sobczyk, *Statystyka*: Podstawy teoretyczne, przykłady, zadania, Wydawnictwo UMCS, Lublin 2000, s. 240.
[3] A. Maksimowicz-Ajchel, *Wstęp do statystyki: Metody opisu statystycznego,* Wydawnictwo Uniwersytetu Warszawskiego, Warszawa 2007, s. 167.

- |0,8-1,0|-współzależność bardzo silna[1].

Współczynnik determinacji jest obliczany, jako kwadrat współczynnika korelacji liniowej Pearsona i informuje o tym, jaka część zmian zmiennej objaśnianej (skutek) jest wyjaśniona przez zmiany zmiennej objaśniającej (przyczyna) w ujęciu procentowym[2].

$$WD=r_{xy}^{2} * 100\%$$

Badana empiryczne zostały przeprowadzone za zgodą władz publicznej uczelni wyższej zgodnie z ogólnie przyjętymi zasadami przeprowadzania badań z zachowaniem pełnej anonimowości respondentów. W celu przeprowadzenia badań empirycznych wykorzystano **kwestionariusz ankiety**:

- załącznik 1 – kwestionariusz dla nauczyciela akademickiego, kadry administracyjnej, studentów (różnych kierunków);
- załącznik 2 – kwestionariusz wywiadu eksperckiego, ma on charakter przekrojowy i posłużył do rozwiązania kilku problemów szczegółowych w pracy doktorskiej.

Podjęte były starania, aby ułożone pytania nie sprawiały respondentom trudności, aby były logiczne, precyzyjne, treściwe, co miało w zamyśle uzyskanie jak najwięcej informacji pod kątem weryfikacji przyjętych hipotez oraz przydatności przy formułowaniu wniosków.

Kwestionariusz ankiety składał się z 20 pytań, w tym 1 pytanie posiadało formę pytania otwartego, a 19 pytań to pytania zamknięte. Pytania w kwestionariuszu wymagały wyboru jednej lub kilku odpowiedzi bądź wymogiem było ustalenie rang poszczególnych odpowiedzi.

Pytania zawarte w kwestionariuszu miały na celu:

- **Pytanie 1** – ustalenie najczęstszego kanału obiegu informacji, z jakiego korzystają respondenci;
- **Pytanie 2-9** – ustalenie opinii respondentów w zakresie bezpieczeństwa systemu informacyjnego;
- **Pytanie 10** – określenie przez respondentów częstotliwości korzystania z konta systemu informatycznego;
- **Pytanie 11** – ustalenie poglądu respondentów na temat charakteru korzystania z systemu informacyjnego w uczelni wyższej;

[1] B. Pułaska-Turyna, *Statystyka dla ekonomistów,* Wydanie II rozszerzone, Difin, Warszawa 2008, s. 275.
[2] M. Sobczyk, *Statystyka…dz. cyt*., s. 239.

- **Pytanie 12** – ustalenie poglądu respondentów na temat bezpieczeństwa danych w systemie informacyjnym w uczelni wyższej;
- **Pytanie 13** – ustalające pogląd respondentów na temat zagrożeń systemu informacyjnego w uczelni wyższej;
- **Pytanie 14** – ustalenie poglądu respondentów na temat odbiorców informacji w systemie;
- **Pytanie 15** – potwierdzenie przez respondentów możliwości w celu zwiększenia poziomu bezpieczeństwa systemu informacyjnego w uczelni wyższej;
- **Pytanie 16** – ustalające pogląd respondentów na temat problemów związanych ze sprawnym działaniem systemu informacyjnego w uczelni wyższej;
- **Pytanie 17** – ustalenie poglądu respondentów na temat stopnia oceny bezpieczeństwa systemu informacyjnego w uczelni wyższej;
- **Pytanie 18** – ustalenie przez respondentów treści przekazywanych telefonicznym kanałem komunikacji;
- **Pytanie 19** – ustalenie opinii respondentów na temat korzystania z pamięci zewnętrznych;
- **Pytanie 20** – potwierdzenie przez respondentów proponowanych zmian w celu zwiększenia poziomu bezpieczeństwa systemu informacyjnego w uczelni wyższej.

Pytanie 20 to pytanie otwarte pozwalające respondentom na wyrażenie indywidualnej opinii do badanych problemów. W ankiecie zostały zawarte także pytania metryczkowe umożliwiające identyfikację respondentów odnośnie wieku, płci, posiadanych stopni naukowych/tytułów, wykształcenia w przypadku kadry administracyjnej, stażu pracy na uczelni wyższej. Metryczka w przypadku studentów zawiera wiek, płeć, stopień studiów, formę kształcenia.

W kwestionariuszu ankiety zastosowano trzy skale pomiarowe. W pytaniu 1 zastosowano skalę pięciostopniową celem ustalenia najczęstszego kanału obiegu informacji w uczelni wyższej. W pytaniach 2-19 oraz w pytaniach metryczkowych zastosowano nominalną skalę pomiarową w odniesieniu do oceny respondentów bezpieczeństwa systemu informacyjnego w uczelni wyższej, korzystania z konta systemu informatycznego jak również problemów związanych z działaniem systemu informacyjnego w uczelni wyższej. W pytaniu 20 zastosowano skalę opisową w celu ustalenia, jakich zmian oczekują respondenci służących zwiększeniu poziomu bezpieczeństwa systemu informacyjnego

w uczelni wyższej. Kwestionariusz ekspercki składał się z 6 pytań, zastosowano skalę opisową.

Pytania w kwestionariuszu dotyczyły:

- **Pytanie 1** – dostosowania organizacji i zasad użytkowania systemu informacyjnego w uczelni wyższej do wymagań współczesnych;
- **Pytanie 2 – 3** – efektywności zarządzania uczelnią wyższą;
- **Pytanie 4** – zagrożeń bezpieczeństwa systemu informacyjnego w uczelni wyższej;
- **Pytanie 5** – uwarunkowania dotyczące bezpieczeństwa systemu informacyjnego w uczelni wyższej
- **Pytanie 6** – wprowadzenie zmian dotyczących bezpieczeństwa systemu informacyjnego w uczelni wyższej.

W procesie badawczym zastosowano i wykorzystano również metodę obserwacji bezpośredniej organizacji i funkcjonowania publicznej uczelni wyższej. Prezentowane wyniki w arkuszu obserwacji[1] były zaczątkiem do podjęcia badań nad problematyką i bezpośrednio wpłynęły na wybór obszaru badań. Arkusz obserwacji pozwolił na weryfikację przyjętej hipotezy potrzeby zmian, jakie należy wprowadzić w bezpieczeństwie systemu informacyjnego w uczelni wyższej, aby poprawić skuteczność ochrony informacji.

1.6. Dobór i charakterystyka próby badawczej

Badania empiryczne sprowadzały się do opinii nauczycieli akademickich, kadry administracyjnej i studentów (różnych kierunków) na temat bezpieczeństwa systemu informacyjnego w organizacji publicznej, jaką jest uczelnia wyższa. Zatem dokonano podziału respondentów na trzy grupy:

- nauczyciele akademiccy,
- kadra administracyjna,
- studenci (różne kierunki).

Dobór próby badawczej na potrzeby przeprowadzenia badań ankietowych został przeprowadzony sposobem doboru losowego prostego zależnego, który umożliwił uzyskanie próby reprezentatywnej. Polegał na bezpośrednim i nieograniczonym doborze jednostek badania do próby statystycznej, gdzie nie jest realizowane zwracanie, z powrotem

[1] Szerzej w zał. 3 arkusz obserwacji bezpośredniej funkcjonowania publicznej uczelni wyższej.

do populacji, wylosowanej jednostki. Sposób ten powoduje, że jednostki badawcze w badaniu mogły uczestniczyć tylko jeden raz[1]. Określenie liczebności próby badawczej uwarunkowane było zarówno wielkością badanej populacji oraz dążeniem do uzyskania precyzyjnych, wiarygodnych, poprawnych wyników wiec liczebność próby została określona, jako wyższa niż 100 jednostek[2].

Badania zostały przeprowadzone w pierwszej połowie roku akademickiego 2023/2024 (semestr zimowy). Badana tematyka była rozpatrzona z perspektywy doświadczonych respondentów, nauczycieli akademickich, pracowników administracji i studentów uczelni wyższej.

Pierwsza grupa to nauczyciele akademiccy w liczbie 500 osób, druga grupa to kadra administracyjna w liczbie 500 osób, w trzeciej grupie znaleźli się studenci podzieleni na stopnie i kierunki, na jakich się kształcą. Łącznie w badaniach ankietowych **wzięło udział 1500 respondentów**, wśród badanych było 1137 kobiet i 363 mężczyzn.

W podziale na grupy to:

- nauczyciele akademiccy – kobiety 298, mężczyźni 202;
- kadra administracyjna – kobiety 458, mężczyźni 42;
- studenci (różne kierunki) – kobiety 381, mężczyźni 119.

Tabela 1.1. Ilościowe zestawienie ankietowanych grup badanych pod względem płci

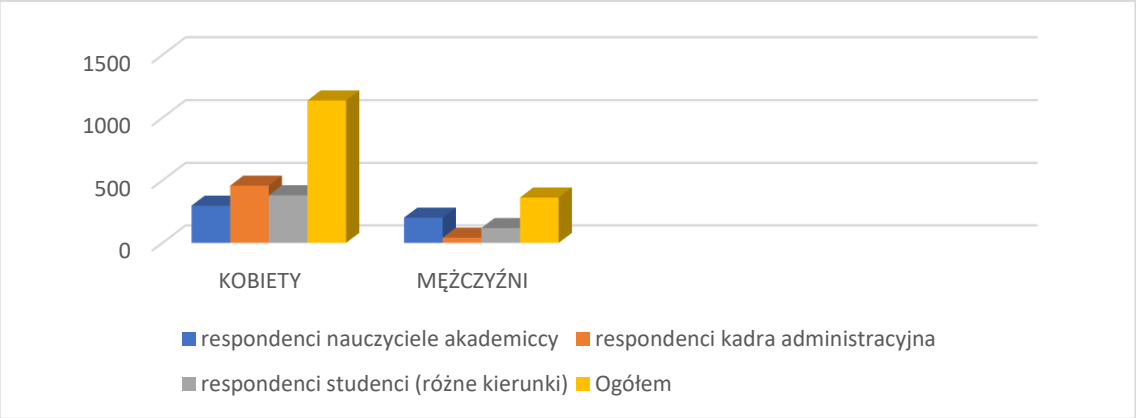
Osoby poddane badaniu	**Respondenci nauczyciele akademiccy**		**Respondenci kadra administracyjna**		**Respondenci studenci (różne kierunki)**		**Ogółem**	
Płeć	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***
KOBIETY	298	59,6%	458	91,6%	381	76,2%	1137	75,8%
MĘŻCZYŹNI	202	40,4%	42	8,4%	119	23,8%	363	24,2%
	500	**100%**	**500**	**100%**	**500**	**100%**	**1500**	**100%**

Źródło: opracowanie własne na podstawie badań własnych

[1] M. Cieślarczyk, *Metody, techniki i narzędzia badawcze oraz elementy statystyki stosowane w pracach magisterskich i doktorskich*, AON, Warszawa 2006, s. 72.

[2] M. Łobocki, *Ustalania liczebności próby badawczej zobacz: Wprowadzenie do metodologii badań pedagogicznych, Oficyna Wydawnicza Impuls*, Warszawa 2010; T. Pilch, *Zasady badań pedagogicznych,* Żak Wydawnictwo Akademickie, Warszawa 1995; B. Walasek-Jarosz, Tok realizacji badań oraz opracowanie wyników, [w:] *Podstawy metodologii badań w pedagogice,* red. S. Palka, GWP, Gdańsk 2010, s. 177–199.

Wykres 1.1. Ilościowe zestawienie ankietowanych grup badanych pod względem płci



Źródło: opracowanie własne na podstawie badań własnych

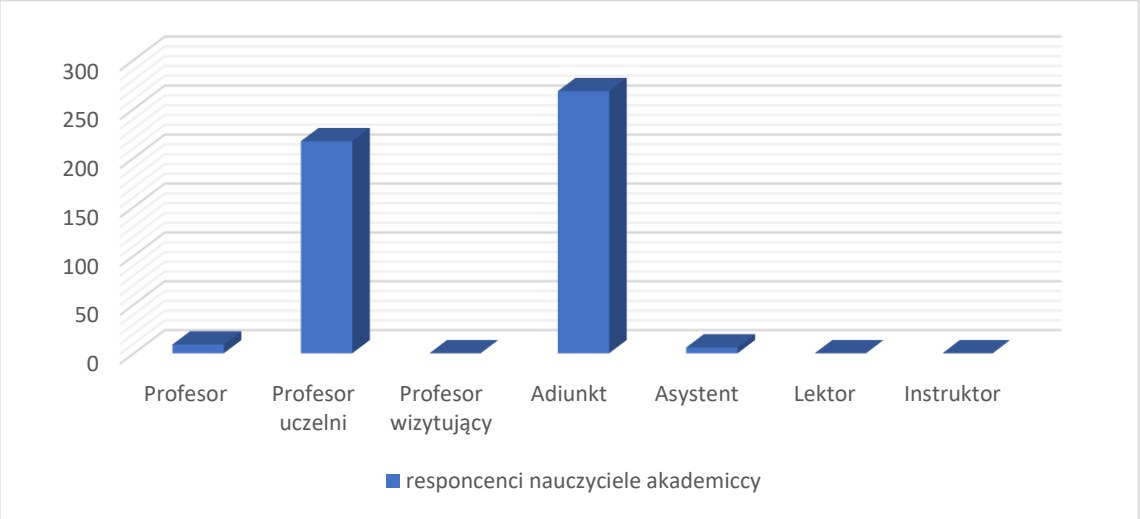
Wśród respondentów dominuje płeć żeńska, takie zróżnicowanie wynika ze specyfiki środowiska uczelnianego, gdzie pracę w zawodzie nauczyciela akademickiego najczęściej podejmują kobiety oraz przez wzgląd na profile kształcenia. W tabeli 1.2. w przypadku nauczycieli akademickich został wskazany rozkład wykształcenia z podziałem na stopnie naukowe i tytuły naukowe.

Tabela 1.2. Charakterystyka respondentów grupy nauczyciele akademiccy pod względem wykształcenia z podziałem na stopnie naukowe i tytuły naukowe (kadra badawczo-dydaktyczna, dydaktyczna

Osoby poddane badaniu	**Respondenci nauczyciele akademiccy**	
stanowiska	*liczba wskazań*	*udział procentowy*
Profesor	9	1,8%
Profesor uczelni	217	43,4%
Profesor wizytujący	0	0%
Adiunkt	268	53,6%
Asystent	6	1,2%
Lektor	0	0%
Instruktor	0	0%
	500	**100%**

Źródło: opracowanie własne na podstawie badań własnych

Wykres 1.2. Charakterystyka respondentów grupy nauczyciele akademiccy pod względem wykształcenia z podziałem na stopnie naukowe i tytuły naukowe (kadra badawczo-dydaktyczna, dydaktyczna)



Źródło: opracowanie własne na podstawie badań własnych

Podając pod uwagę uzyskane wyniki badań, jednoznacznie należy stwierdzić, że wśród respondentów grupy nauczycieli akademickich było najwięcej nauczycieli zajmujących stanowisko adiunkta 53,6%. Na kolejnym miejscu uklasyfikowali się nauczyciele akademiccy posiadający stopień naukowy dr hab. i zajmujący stanowisko profesora uczelni. Taki podział wynika z dużej ilości zatrudnionych osób ze stopniem doktora.
W tabeli 1.3. został przedstawiony podział rozłożonych odpowiedzi pod względem charakterystyki respondentów grupy nauczyciele akademiccy pod względem wykształcenia z podziałem na stopnie naukowe i tytuły naukowe (kadra badawczo-dydaktyczna, dydaktyczna) z podziałem na płeć.

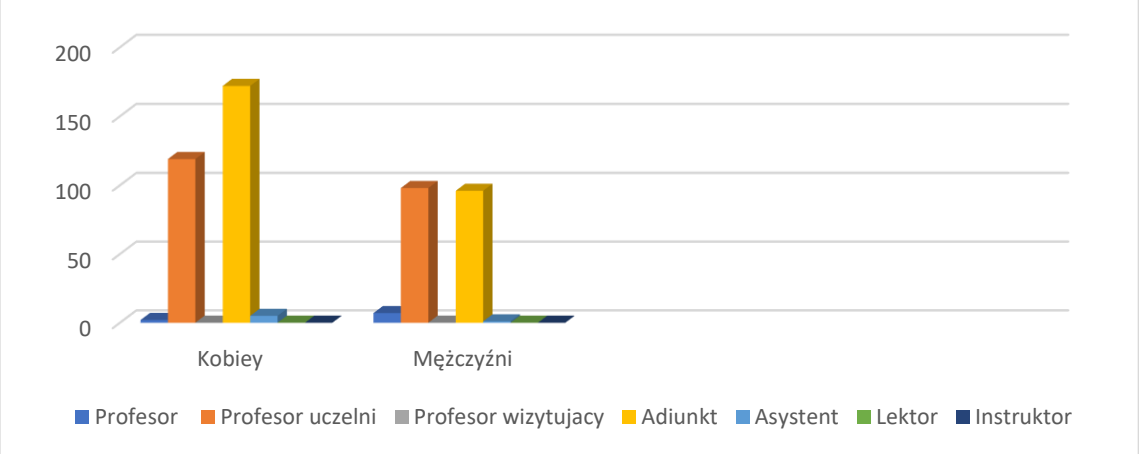
Tabela 1.3. Charakterystyka respondentów grupy nauczyciele akademiccy pod względem wykształcenia z podziałem na stopnie naukowe i tytuły naukowe (kadra badawczo-dydaktyczna, dydaktyczna) z podziałem na płeć

Osoby poddane badaniu			
Respondenci nauczyciele akademiccy			
stanowiska	**płeć**	***liczba wskazań***	***udział procentowy***
Profesor	**KOBIETA**	2	0,4%
	MĘŻCZYZNA	7	1,4%

Profesor uczelni	**KOBIETA**	119	23,8%
	MĘŻCZYZNA	98	19,6%
Profesor wizytujący	**KOBIETA**	0	0%
	MĘŻCZYZNA	0	0%
Adiunkt	**KOBIETA**	172	34,4%
	MĘŻCZYZNA	96	19,2%
Asystent	**KOBIETA**	5	1%
	MĘŻCZYZNA	1	0,2%
Lektor	**KOBIETA**	0	0%
	MĘŻCZYZNA	0	0%
Instruktor	**KOBIETA**	0	0%
	MĘŻCZYZNA	0	0%
		500	**100%**

Źródło: opracowanie własne na podstawie badań własnych

Wykres 1.3. Charakterystyka respondentów grupy nauczyciele akademiccy pod względem wykształcenia z podziałem na stopnie naukowe i tytuły naukowe (kadra badawczo-dydaktyczna, dydaktyczna) z podziałem na płeć



Źródło: opracowanie własne na podstawie badań własnych

W tabeli 1.4. został przedstawiony podział nauczycieli akademickich ze względu na staż pracy i płeć.

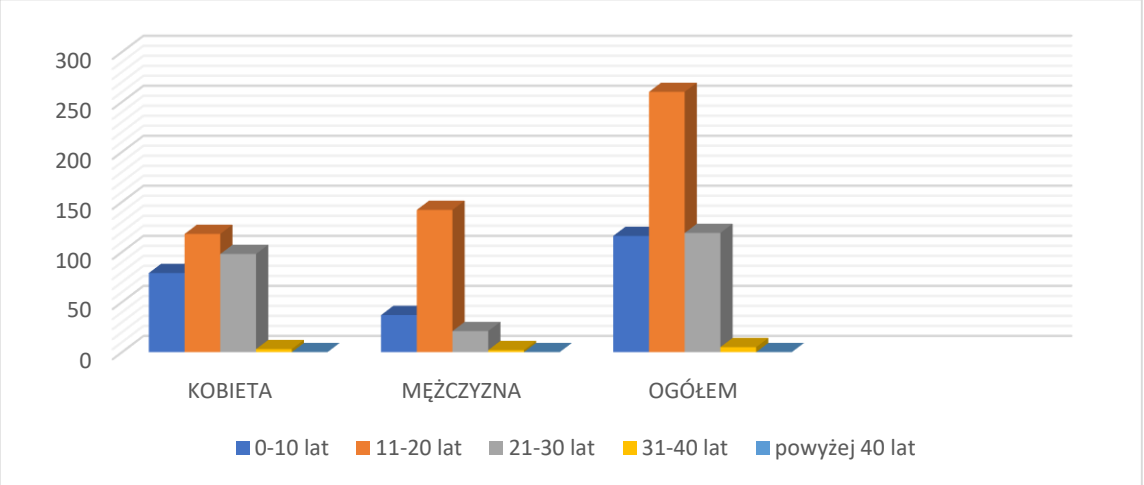
Tabela 1.4. Charakterystyka respondentów grupy nauczyciele akademiccy pod względem stażu pracy i płci

Osoby poddane badaniu			
Respondenci nauczyciele akademiccy			
lata	**płeć**	***liczba wskazań***	***udział procentowy***
0-10	**KOBIETA**	79	15,8%
	MĘŻCZYZNA	37	7,4%

11-20	**KOBIETA**	118	23,6%
	MĘŻCZYZNA	142	28,4%
21-30	**KOBIETA**	98	19,6%
	MĘŻCZYZNA	21	14,2%
31-40	**KOBIETA**	3	0,6%
	MĘŻCZYZNA	2	0,4%
Powyżej 40	**KOBIETA**	0	0%
	MĘŻCZYZNA	0	0%
		500	**100%**

Źródło: opracowanie własne na podstawie badań własnych

Wykres 1.4. Charakterystyka respondentów grupy nauczyciele akademiccy pod względem stażu pracy i płci



Źródło: opracowanie własne na podstawie badań własnych

Dokonując analizy uzyskanych wyników najliczniejszą grupą wśród zatrudnionych nauczycieli akademickich są kobiety posiadające staż pracy 11-20 lat. Wśród mężczyzn dominuje ten sam przedział lat pracy, co zadeklarowany przez kobiety. Nikt z respondentów nie wskazał na staż pracy wyższy niż 40 lat. Badanie wskazuje, że kadra nauczycieli akademickich powinna wyróżniać się dojrzałością i przez lata nabytym doświadczeniem jak i wysokimi kompetencjami w pracy zawodowej. Wspomniana sytuacja powinna mieć przełożenie na właściwe i poprawne wypełnienie kwestionariusza ankiety a tym samym, wykazanie się szeroką wiedzą i praktyką. Kolejna grupa poddana badaniu to grupa reprezentująca kadrę administracyjną.

W tabeli 1.5. została zaprezentowana charakterystyka respondentów grupy kadra administracyjna pod względem wykształcenia.

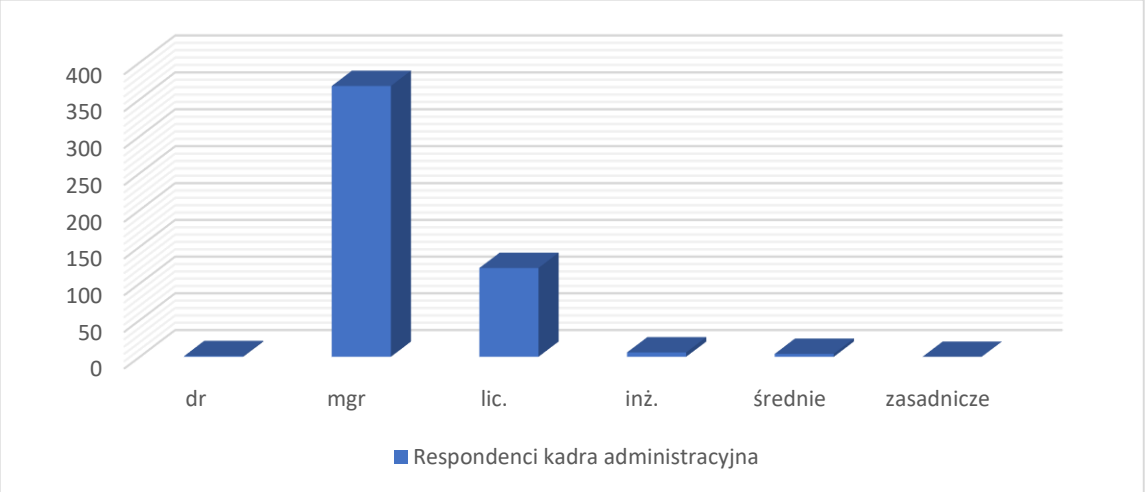
Tabela 1.5. Charakterystyka respondentów grupy kadra administracyjna pod względem wykształcenia

Osoby poddane badaniu		**Respondenci kadra administracyjna**	
wykształcenie		*liczba wskazań*	*udział procentowy*
dr		1	0,2%
wyższe	**mgr**	368	73,6%
	lic.	121	24,2%
	inż.	6	1,2%
średnie		4	0,8%
zasadnicze		0	0%
		500	**100%**

Źródło: opracowanie własne na podstawie badań własnych

W ocenie uzyskanych wyników widać, że duża część kadry administracyjnej posiada wykształcenie wyższe mgr jest to 368 osób, w przeliczeniu procentowym wychodzi 73,2% społeczności poddanej badaniu. Drugim w kolejności tytułem naukowym nadanym przez uczelnię jest licencjat, i tu zadeklarowało 24,2% respondentów. Wykształcenie zasadnicze nie zostało zadeklarowane w tym przypadku przez żadnego pracownika zatrudnionego na stanowisku kadry administracyjnej.

Wykres 1.5. Charakterystyka respondentów grupy kadra administracyjna pod względem wykształcenia



Źródło: opracowanie własne na podstawie badań własnych

Poniżej została przedstawiona tabela 1.6. w której zawiera się charakterystyka respondentów grupy kadra administracyjna zawierająca takie informacje jak, wykształcenie z podziałem na płeć.

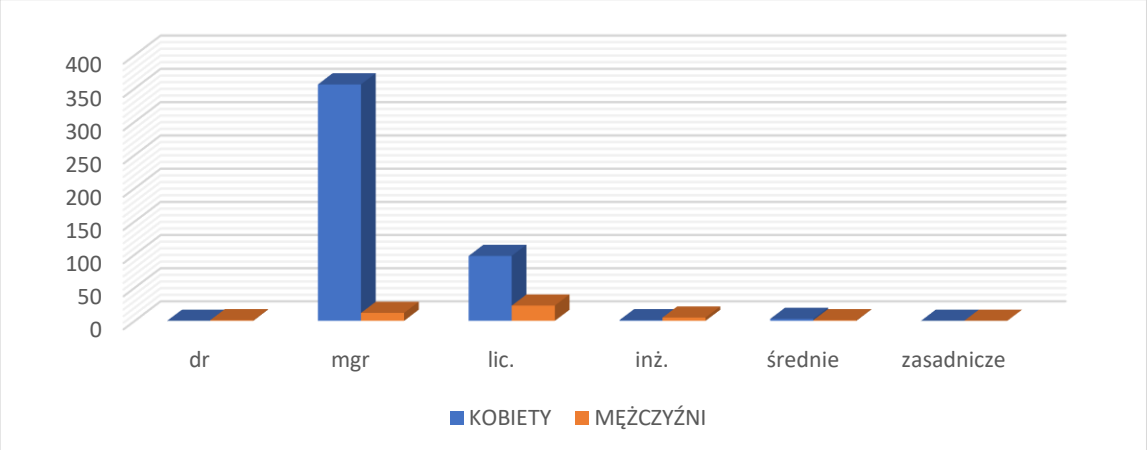
Tabela 1.6. Charakterystyka respondentów grupy kadra administracyjna ze względu na wykształcenie i płeć

Osoby poddane badaniu			**Respondenci kadra administracyjna**	
wykształcenie		**płeć**	*liczba wskazań*	*udział procentowy*
dr		**KOBIETY**	0	0%
		MĘŻCZYŹNI	1	0,2%
wyższe	**mgr**	**KOBIETY**	356	71,2%
		MĘŻCZYŹNI	12	2,4%
	lic.	**KOBIETY**	98	19,6%
		MĘŻCZYŹNI	23	4,6%
	inż.	**KOBIETY**	1	0,2%
		MĘŻCZYŹNI	5	1%
średnie		**KOBIETY**	3	0,6%
		MĘŻCZYŹNI	1	0,2%
zasadnicze		**KOBIETY**	0	0%
		MĘŻCZYŹNI	0	0%
			500	**100%**

Źródło: opracowanie własne na podstawie badań własnych

W ocenie uzyskanych badań należy stwierdzić, że wykształcenie wyższe z tytułem naukowym nadanym przez uczelnie (mgr) wśród respondentów (kobiet) posiada 356 osób to w przeliczeniu procentowym wynosi 71,2%. Mężczyźni posiadający ten sam tytuł i są w ilości 12 osób a w przeliczeniu procentowym to 2,4%. Wykształcenie wyższe (licencjat) deklaruje 19,6% kobiet i 4,6% mężczyzn.

Wykres 1.6. Charakterystyka respondentów grupy kadra administracyjna ze względu na wykształcenia i płeć



Źródło: opracowanie własne na podstawie badań własnych

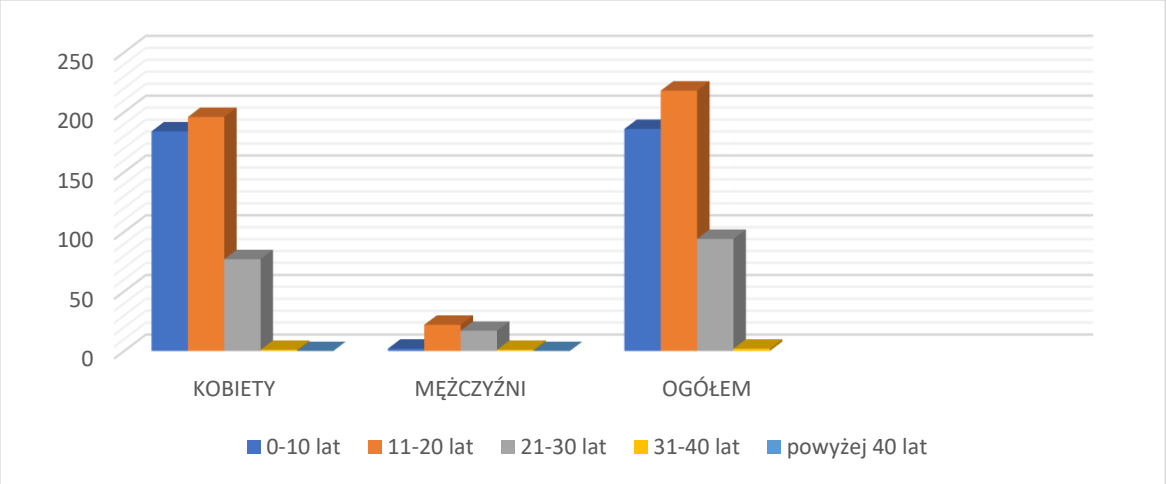
W tabeli 1.7. została przedstawiona charakterystyka respondentów grupy kadra administracyjna pod względem stażu pracy i płci.

Tabela 1.7. Charakterystyka respondentów grupy kadra administracyjna pod względem stażu pracy i płci

Osoby poddane badaniu			
Respondenci kadra administracyjna			
lata	**płeć**	***liczba wskazań***	***udział procentowy***
0-10	**KOBIETA**	184	36,8%
	MĘŻCZYZNA	2	0,4%
11-20	**KOBIETA**	196	39,2%
	MĘŻCZYZNA	22	4,4%
21-30	**KOBIETA**	77	15,4%
	MĘŻCZYZNA	17	3,4%
31-40	**KOBIETA**	1	0,2%
	MĘŻCZYZNA	1	0,2%
Powyżej 40	**KOBIETA**	0	0%
	MĘŻCZYZNA	0	0%
		500	**100%**

Źródło: opracowanie własne na podstawie badań własnych

Wykres 1.7. Charakterystyka respondentów grupy kadra administracyjna pod względem stażu pracy i płci



Źródło: opracowanie własne na podstawie badań własnych

Dokonując analizy uzyskanych wyników najliczniejszą grupą wśród zatrudnionych na stanowisku kadry administracyjnej są kobiety posiadające staż pracy 11-20 lat. Wśród mężczyzn dominuje ten sam przedział lat pracy, co zadeklarowany przez kobiety. Nikt z respondentów nie wskazał na staż pracy wyższy niż 40 lat. Badanie wskazuje, że

kadra administracyjna powinna wyróżniać się dojrzałością i przez lata nabytym doświadczeniem jak i wysokimi kompetencjami w pracy zawodowej. Wspomniana sytuacja powinna mieć przełożenie na właściwe i poprawne wypełnienie kwestionariusza ankiety a tym samym, wykazanie się szeroką wiedzą i praktyką. Wśród kobiet staż pracy 11-20 lat zadeklarowało 196 kobiet, co w przeliczeniu procentowym daje 39,2 % oraz 22 mężczyzn, co w przeliczeniu procentowym daje 4,4%. Ostatnią grupą respondentów są studenci (różne kierunki), a charakterystyka respondentów tej grupy pod względem stopnia i formy realizacji studiów przedstawia tabela 1.8.

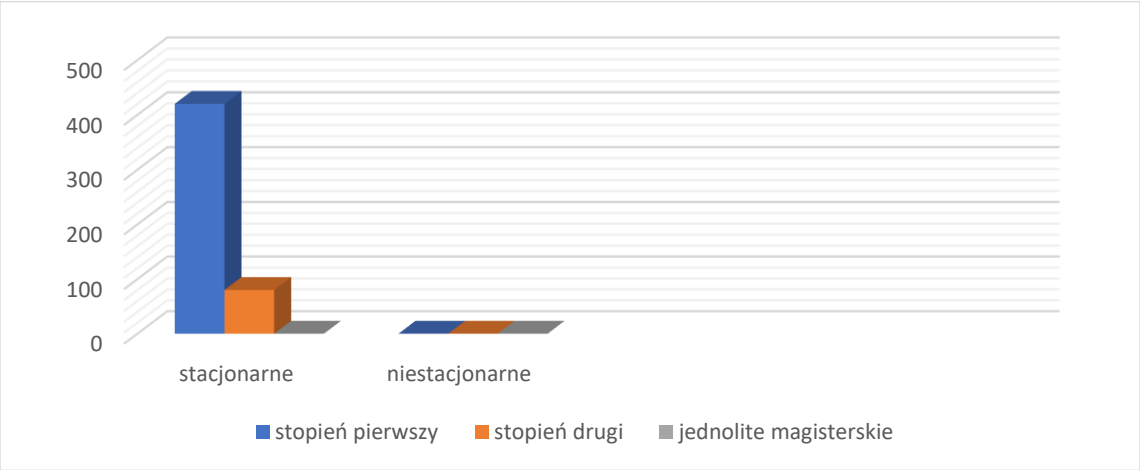
Tabela 1.8. Charakterystyka respondentów grupy studenci (różne kierunki) pod względem stopnia i formy realizacji studiów

Osoby poddane badaniu		**Respondenci studenci (różne kierunki)**	
Wykształcenie		*liczba wskazań*	*udział procentowy*
Stopień	**Forma kształcenia**		
pierwszy	**stacjonarne**	420	84%
	niestacjonarne	0	0%
drugi	**stacjonarne**	80	16%
	niestacjonarne	0	0%
jednolite magisterskie	**stacjonarne**	0	0%
	niestacjonarne	0	0%
		500	**100%**

Źródło: opracowanie własne na podstawie badań własnych

Analiza danych wykazała, że najliczniejszą grupą studentów, respondentów są studenci pierwszego stopnia studiów stacjonarnych 420 osób, co w przeliczeniu procentowym wynosi 84%. Kształcenie na drugim stopniu zadeklarowało 80 osób, co w przeliczeniu procentowym daje 16%. Studenci pierwszego stopnia są najliczniejszą grupą studentów, ponieważ zwykle studia drugiego stopnia są studiami uzupełniającymi, więc jest mniejszy odsetek osób chcących podjąć dalsze kształcenie.

Wykres 1.8. Charakterystyka respondentów grupy studenci (różne kierunki) pod względem stopnia i formy realizacji studiów



Źródło: opracowanie własne na podstawie badań własnych

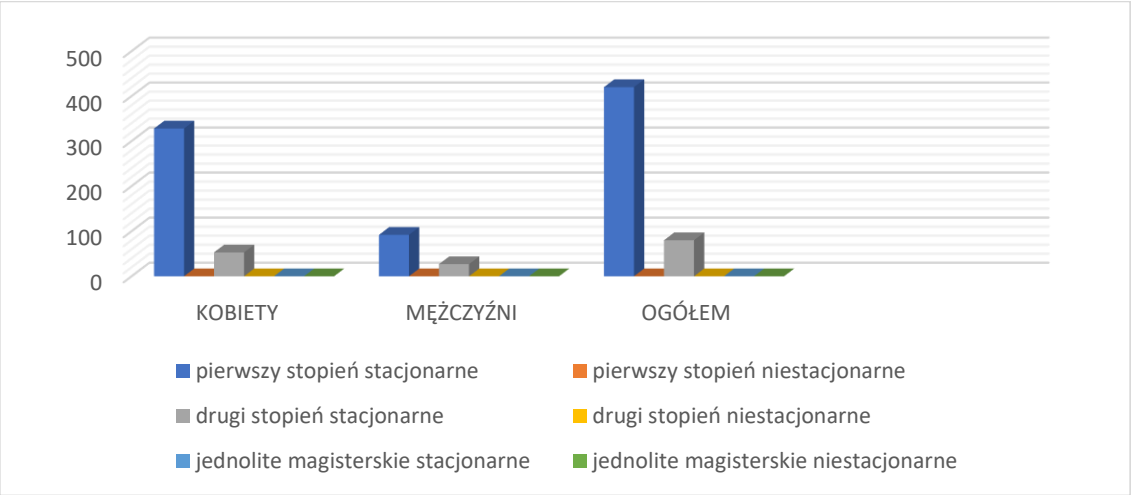
W tabeli 1.9. została przedstawiona charakterystyka respondentów grupy studentów (różne kierunki) pod względem formy i realizacji studiów z podziałem na płeć.

Tabela 1.9. Charakterystyka respondentów grupy studentów (różne kierunki) pod względem formy i realizacji studiów z podziałem na płeć

Osoby poddane badaniu			**Respondenci studenci**	
Wykształcenie			*liczba wskazań*	*udział procentowy*
Stopień	**Forma kształcenia**			
pierwszy	**stacjonarne**	**KOBIETY**	328	65,6%
		MĘŻCZYŹNI	92	18,4%
	niestacjo-narne	**KOBIETY**	0	0%
		MĘŻCZYŹNI	0	0%
drugi	**stacjonarne**	**KOBIETY**	53	10,6%
		MĘŻCZYŹNI	27	5,4%
	niestacjo-narne	**KOBIETY**	0	0%
		MĘŻCZYŹNI	0	0%
jednolite magi-sterskie	**stacjonarne**	**KOBIETY**	0	0%
		MĘŻCZYŹNI	0	0%
	niestacjo-narne	**KOBIETY**	0	0%
		MĘŻCZYŹNI	0	0%
			500	**100%**

Źródło: opracowanie własne na podstawie badań własnych

Wykres 1.9. Charakterystyka respondentów grupy studentów (różne kierunki) pod względem formy i realizacji studiów z podziałem na płeć



Źródło: opracowanie własne na podstawie badań własnych

Z przeprowadzonej analizy wynika, że to kobiety były w większości grupą, która uczestniczyła w badaniach i wypełniała kwestionariusz ankiety. Studentów płci żeńskiej było 381 kobiet. Respondentów pierwszego stopnia płci żeńskiej, odpowiadających na pytania było 328 osób, co w przeliczeniu procentowym wdało 65,6% a na drugim stopniu 53 osoby tej samej płci, co w przeliczeniu procentowym 10,6%. W udzielaniu odpowiedzi wzięli także udział respondenci płci męskiej stopnia pierwszego w liczbie 92 osoby to w przeliczeniu procentowym wynosi 18,4%, zaś na drugim stopniu wypowiedziało się 27 mężczyzn, co w przeliczeniu procentowym wynosi 5,4%. W badaniu wzięli udział studenci i studentki studiów stacjonarnych. Studenci kształcący się na studiach niestacjonarnych oraz jednolitych magisterskich nie brali udziału w badaniach. Tabela 1.10. zawiera trzy grupy respondentów z podziałem na wiek i płeć.

Tabela 1.10. Charakterystyka respondentów z podziałem na wiek i płeć

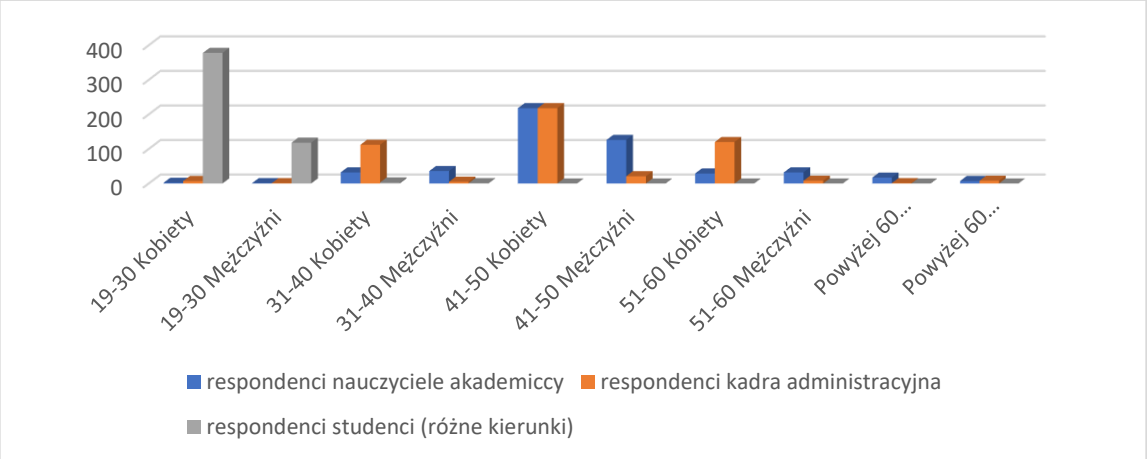
Osoby poddane badaniu		**Respondenci nauczyciele akademiccy**		**Respondenci kadra administracyjna**		**Respondenci studenci (różne kierunki)**		**Ogólem**	
wiek	**płeć**	*liczba wskazań*	*udział procentowy*	*liczba wskazań*	*udział procentowy*	*liczba wskazań*	*udział procentowy*	*liczba wskazań*	*udział procentowy*
19-30	**KOBIETA**	2	0,4%	7	1,4%	378	75,6%	387	25,8%
	MĘŻCYZNA	1	0,2%	1	0,2%	118	23,6%	120	8%
31-40	**KOBIETA**	32	6,4%	112	22,4%	3	0,6%	147	9,8%
	MĘŻCZYZNA	36	7,2%	5	1%	1	0,2%	42	2,8%
41-50	**KOBIETA**	218	43,6%	218	43,6%	0	0%	436	29,07%

	MĘŻCZY-ZNA	126	25,2%	21	4,2%	0	0%	147	9,8%
51-60	**KOBIETA**	29	5,8%	120	24%	0	0%	149	9,9%
	MĘŻCZY-ZNA	32	6,4%	8	1,6%	0	0%	40	2,63%
Powyżej 60	**KOBIETA**	17	3,4%	1	0,2%	0	0%	18	1,2%
	MĘŻCZY-ZNA	7	1,4%	8	1,6%	0	0%	15	1%
		500	**100%**	**500**	**100%**	**500**	**100%**	**1500**	**100%**

Źródło: opracowanie własne na przykładzie badań własnych

Analiza pozyskanych odpowiedzi wskazuje, że w grupie nauczycieli akademickich najwięcej odpowiedzi udzieliło respondentów w przedziale wiekowym 41-50 lat, tak samo jak to było uwidocznione w przypadku kadry administracyjnej co dało 43,6%. Studenci udzielający odpowiedzi deklarowali przedział największy 19-30 lat w przeliczeniu procentowym to 75,6%. Tak duża ilość studentów w tym przedziale może świadczyć o tym, że odpowiedzi udzielali tylko studenci, którzy studiują stacjonarnie w związku z powyższym najczęściej są to osoby właśnie w takim wieku.

Wykres 1.10. Charakterystyka respondentów z podziałem na wiek i płeć



Źródło: opracowanie własne na podstawie badań własnych

1.7. Ogólna charakterystyka terenu badań

Prace badawcze na potrzeby dysertacji zostały przeprowadzone w organizacji o charakterze publicznym. Jest to uczelnia wyższa z długoletnią tradycją o bogatej historii, o czym mówi dokumentacja źródłowa. W ofercie uczelni jest szeroka oferta kierunków studiów pierwszego, drugiego stopnia oraz jednolitych magisterskich. Odbywa się także kształcenie studentów na studiach podyplomowych. Uczelnia wyższa realizuje

swoje cele i zadania wynikające z Ustawy *Prawo o szkolnictwie wyższym i nauce*, odniesienie zasad i celów można znaleźć w statucie uczelni, uchwałach, decyzjach, zarządzeniach. Uczelnia kieruje się podstawowymi zadaniami tj:

- prowadzeniem kształcenia na studiach wyższych, podyplomowych lub innych form kształcenia;
- poprowadzi działalność naukową, świadczy usługi badawcze i transfer wiedzy oraz technologii do gospodarki;
- prowadzi kształcenie doktorantów, kształcenie i promowanie kadr uczelni;
- stwarza osobom niepełnosprawnym odpowiednie warunki do udziału w procesie przyjmowania na uczelnię, kształcenia, prowadzenia działalności naukowej;
- wychowuje studentów mających następnie poczucie odpowiedzialności za polskie państwo, narodową tradycję, poszanowanie praw człowieka;
- stwarza warunki do rozwoju kultury fizycznej studentów;
- upowszechnia, jak również pomnaża osiągnięcia nauki i kultury poprzez udostępnianie zbiorów naukowych, archiwalnych, bibliotecznych;
- działanie na rzecz lokalnych i regionalnych społeczności[1].

1.8. Charakterystyka procedury badawczej, w tym wskazanie etapów i harmonogramu pracy badawczej

W celu rozwiązania problemów badawczych i weryfikacji przyjętych hipotez, przeprowadzony został proces badawczy składający się z trzech etapów.

Rysunek.1.1. Etapy procesu badawczego

Źródło: opracowanie własne

[1] Ustawa z dnia 20.07.2018 r., *Prawo o szkolnictwie wyższym i nauce* (Dz.U. z 2018 r., poz. 1668)., https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20180001668/U/D20181668Lj.pdf (dostęp: 18.02.2023).

W pierwszej fazie zostały poruszone kwestie dotyczące przedmiotu i celu badań. Został sformułowany problem badawczy, hipotezy robocze i hipotezy szczegółowe. Dokonano wyboru metod, technik, narzędzi badawczych występujących w postaci kwestionariusza ankiety jak i kwestionariusza wywiadu eksperckiego. Przedstawiony został obszar i teren badań następnie została dobrana i scharakteryzowana próba badawcza. Dokonano weryfikacji, analizy literatury badanego przedmiotu, dokonano także przekroju dokumentów normatywnych dotyczących problematyki bezpieczeństwa systemu informacyjnego organizacji publicznej na przykładzie uczelni wyższej. Następnie nastąpiło opracowanie koncepcji rozprawy doktorskiej.

Etap drugi badań polegał na przeprowadzeniu badania empirycznego przy wykorzystaniu kwestionariusza ankiety, arkusza wywiadu. Wykorzystano także metody teoretyczne pozwalające na uzyskanie materiału i wyodrębnieniu składników mających istotne znaczenie w procesie badawczym.

W końcowym już etapie trzecim nastąpiło zwieńczenie czynności procesu badawczego. Nastąpiło to poprzez logiczne uogólnienie, systematyzację zgromadzonego materiału empirycznego i analizę statystyczną. Ten etap to weryfikacja hipotezy głównej, hipotez szczegółowych stanowiących, że obecny system informacyjny w publicznej organizacji na przykładzie uczelni wyższej nie w pełni chroni informację. Koniec został dodatkowo zwieńczony opracowaniem koncepcji bezpieczeństwa systemu informacyjnego w uczelni wyższej. Tabela 1.11. przedstawia proces przebiegu badawczego.

Tabela 1.11. Przebieg procesu badawczego

		Czynności
ETAP 1 Konceptualizacja, badania wstępne	**1.**	Określenie i rozpoznanie problemu badawczego
	2.	Zbieranie informacji wyjściowych poprzez analizę literatury przedmiotu i dokumentów normatywnych
	3.	Opracowanie koncepcji rozprawy doktorskiej • werbalizacja ogólna problemu badawczego • określenie celu i przedmiotu badań • sformułowanie problemów badawczych • sformułowanie hipotez roboczych • dobór metod, technik, narzędzi badawczych
	4.	Dobór próby badawczej
	5.	Przygotowanie narzędzi badawczych: • opracowanie kwestionariusza ankiety • opracowanie kwestionariusza wywiadu

		Czynności
ETAP 2 Badania własne	**6.**	Analiza dostępnych materiałów pod względem: • aktualnego stanu prawnego badanego przedmiotu, jakim jest bezpieczeństwo systemu informacyjnego • doskonalenia kluczowych kompetencji • zagrożeń w systemie bezpieczeństwa informacyjnego w uczelni wyższej
	7.	Ocena stanu prawnego dotyczącego systemu bezpieczeństwa informacji w oparciu o obowiązujące akty prawne
	8.	Analiza przez autorkę kwestionariusza ankiety
	9.	Przeprowadzenie badań empirycznych przy wykorzystaniu: • kwestionariusza ankiety • kwestionariusza wywiadu
ETAP 3 Finalizacja badań	10.	Przygotowanie danych empirycznych do analiz, obliczeń statystycznych
	11.	Analiza jakościowa i ilościowa zebranych danych
	12.	Interpretacja otrzymanych wyników badań teoretycznych, empirycznych w kontekście rozwiązania założonych problemów badawczych
	13.	Weryfikacja hipotez
	14.	Opracowanie koncepcji bezpieczeństwa systemu informacyjnego w uczelni wyższej
	15.	Wnioski końcowe

Źródło: opracowanie na podstawie: M. Cieślarczyk, Metody, techniki i narzędzia badawcze oraz elementy statystyki stosowane w pracach magisterskich i doktorskich, AON, Warszawa 2006, s. 22-24.

2. BEZPIECZEŃSTWO SYSTEMU INFORMACYJNEGO

W oparciu o literaturę przedmiotu jak i doświadczenie w funkcjonowaniu uczelni wyższej, jako organizacji publicznej, dokonana została analiza otoczenia. Problematyka zarządzania informacją znajduje się w zakresie prac naukowo-badawczych, jak i wszelkich publikacji[1]. W tym rozdziale został przybliżony teoretyczny aspekt dotyczący systemu informacyjnego, jako samej informacji oraz bezpieczeństwa w kontekście bezpiecznego jej przepływu, przechowywania. Pod rozwagę zostały wzięte narzędzia, które są wykorzystane podczas jej dystrybucji. Weryfikacji zostały poddane obowiązujące prawne uregulowania a w ramach weryfikacji przyjętych hipotez dokonano diagnozy systemu informacyjnego funkcjonującego w organizacji publicznej na przykładzie publicznej uczelni wyższej.

Celem przedstawionych badań było rozwiązanie szczegółowego problemu badawczego zawartego w pytaniu, *Jakie uwarunkowania wpływają na bezpieczeństwo systemu informacyjnego w uczelni wyższej?* Jak również w dalszej części przyjętej hipotezy, stanowiącej przypuszczenie, iż *bezpieczeństwo systemu informacyjnego w uczelni wyższej regulowane jest pośrednio i bezpośrednio źródłami powszechnie obowiązującego prawa w RP*. Do takich źródeł należą Konstytucja RP, ratyfikowane umowy międzynarodowe, ustawy, rozporządzenia oraz akta prawa miejscowego mające w swoim zasięgiem obszar działania organów, które je ustanowiły.

Informacja traktowana jest, jako zasób i narzędzie stanowiące podstawę działalności analitycznej. Bez informacji i jej właściwego przekazywania w systemie nie ma szans na poprawne, efektywne, szybkie wykorzystanie działalności analitycznej mającej na celu zwiększenie bezpieczeństwa zarówno samych obywateli a w szczególności państwa[2]. *Bezpieczeństwo systemu informacyjnego przekłada się na bezpieczeństwo interesariuszy uczelni i świadczy o wysokim standardzie zarządzania jednostką organizacyjną*.

Uczelnia jest też organizacją publiczną świadczącą najwyższej, jakości kształcenie studentów na wszystkich kierunkach oraz prowadzi działalność naukową wpływającą na rozwój społeczny. W celu rozwiązania wskazanego problemu badawczego i weryfikacji sformułowanej hipotezy zastosowano następujące metody badawcze:

[1] H. Bieniok, *Metody sprawnego zarządzania. Planowanie, organizowanie, motywowanie, kontrola,* AW, Warszawa 1997, s. 12.
[2] K. Liedel, P. Piasecka, T. R. Aleksandrowicz, *Analiza…dz. cyt.,* s. 33.

- *analiza* – została zastosowana do weryfikacji literatury specjalistycznej przedmiotu, aktów normatywnych jak i dokumentacji uczelnianej;
- *synteza* – została wykorzystana do poznania istoty zjawiska jak również scalenia pozyskanych wyników analizy w jedną syntetyczną całość;
- *abstrahowanie* – metoda ta została wykorzystana podczas wyodrębniania elementów przedmiotu badań, uznanych za drugorzędne i nieistotne[1];
- *uogólnienie* – zastosowano przy określeniu poziomu bezpieczeństwa badanego systemu informacyjnego, uwzględnione zostało środowisko zewnętrzne i wewnętrzne uczelni wyższej a polegało na łączeniu podobnych faktów;
- *porównanie* – miało swoje zastosowanie przy identyfikacji cech wspólnych, różnic, podobieństw i dotyczyło poszczególnych zagadnień badawczych. Szczególnie przydatne było

  w zakresie obiegu informacji oraz bezpieczeństwa tego procesu w organizacji publicznej, uczelni wyższej;
- *wnioskowanie* – wykorzystane we wszystkich rozdziałach znajdujących się w pracy doktorskiej, w części poświęconej wnioskom i w zakończeniu dysertacji;
- *dedukcja* – wykorzystana została do uogólnienia, wskazania wszystkich czynników, które mogą wpłynąć na bezpieczeństwo systemu informacyjnego w uczelni wyższej;
- *redukcja* – miała zastosowanie i przełożyła się na wskazanie i opisanie rezultatów stosowania systemu obiegu informacji w uczelni wyższej, jako organizacji publicznej[2];
- *obserwacja* – została wykorzystana do przemyśleń nad sytuacją problemową a która wychodzi naprzeciw podjętym badaniom i sformułowaniu celu ich prowadzenia a na końcu trafnej analizy i interpretacji;
- *metoda sondażu diagnostycznego* [3] – zastosowana została *technika ankiety,* dzięki niej była możliwość pozyskania opinii respondentów, ich postrzeganie dot. zjawiska badanego. Nastąpiło wykorzystanie *techniki wywiadu eksperckiego*, którego niezmiennym celem było poznanie opinii eksperta w zakresie systemu informacyjnego działającego w uczelni wyższej.

[1] E. Wiśniewski, *Metodyka wojskowych …dz. cyt.*, s. 74.
[2] W. Pytkowski, *Organizacja badań…dz. cyt.*, s. 117-124
[3] J. Apanowicz, *Metodologia nauk, Dom Organizatora,* Toruń 2003, s. 25-51.

2.1. Istota bezpieczeństwa systemu informacyjnego

Prężnie rozwijająca się współczesność oparta na informacji stała się celem nadrzędnym w pozyskiwaniu wszelkich danych z udziałem osób stosujących nielegalne praktyki dla takich pobudek jak zysk, przejęcie władzy, medialność czy chociażby osłabienie bezpieczeństwa państwa. Informacja może przybierać różne formy, co potwierdza PN-ISO/IEC 17799: 2007, może być to forma wydrukowana, odręcznie zapisana na kartce, przesyłana za pośrednictwem poczty zwykłej jak i elektronicznej, przechowywana na nośnikach, komputerach, laptopach (forma elektroniczna) itd..

Wydawać się może, że istotnym będzie spór o zdefiniowanie tego pojęcia[1] jednakże ważniejszy jest jednak fakt, iż rozwój technologii informacyjnych i komunikacyjnych (ICT, ang. i*nformation and communication technologies)* i ich powszechność spowodowała wyjątkową swobodę dostępu, dystrybucji oraz wymiany informacji[2]. Dostępność informacji będąca wynikiem rewolucji informatycznej stworzyła podstawę dla integracji wiedzy, technologii, gospodarki, kultury[3]. W efekcie ewaluując w kierunku społeczeństwa informacyjnego z jego informacją globalną czy gospodarką, niemającego administracyjnych czy organizacyjnych granic terytorialnych[4]. Nie ma znaczenia, jaką formę przybiera informacja jak również za pomocą, jakich środków przekazu jest ona udostępniana jednakże ważne jest, aby zawsze była ona w odpowiedni sposób chroniona przed osobami trzecimi kierującymi się złymi intencjami.

Bezpieczeństwo systemu informacyjnego jest bardzo ważne dla każdego sektora zarówno publicznego jak i prywatnego ma to ogromny wpływ na ochronę infrastruktury krytycznej. Zarówno w jednym jak i drugim sektorze bezpieczeństwo systemu informacyjnego może funkcjonować, jako dźwignia biznesu oraz większej wygody dla społeczności poprzez tworzenie portali e-urzędu lub e-gospodarki czy unikanie bądź redukowanie ryzyka. Przenikanie wspomnianych sieci publicznych i prywatnych, ich współużytkowanie w zakresie informacyjnych zasobów utrudnia w pewnym stopniu utrzymanie kontroli dostępu.

---

[1] M. J. Schroeder, *Spór o pojęcie informacji, „Studia Metodologiczne*", 2015/34, s. 11.
[2] M. Leszczyńska, *Współczesny model rozwoju społecznego z perspektywy rewolucji informacyjnej [w:] Nierówności społeczne a wzrost gospodarczy*. *Społeczeństwo informacyjne – regionalne aspekty rozwoju*, red. M. Woźniak, UR, Rzeszów 2011, s. 129
[3] M. Niezgoda, *Społeczeństwo informacyjne w perspektywie socjologicznej: idea czy rzeczywistość?, [w:] Społeczeństwo informacyjne – wizja czy rzeczywistość,* red. L. Haber, Uczelniane Wydawnictwo Naukowo-Dydaktyczne, Kraków 2003, s. 122.
[4] T. Goban-Klas, P. Sienkiewicz, *Społeczeństwo informacyjne – szanse, zagrożenia, wyzwania*, Wydawnictwo Fundacji Postępu Telekomunikacji, Kraków 1999, s. 78.

Tendencja wprowadzania rozproszonego przetwarzania, osłabia skuteczność centralnych specjalistycznych mechanizmów zarządzania[1]. Państwo troszcząc się o własne bezpieczeństwo ustala pewien zbiór wartości wewnętrznych, mających jego zdaniem chronić przed zagrożeniami. Bezpieczeństwo państwa obejmuje problematykę przeciwstawiania się występującym zagrożeniom wewnętrznym i zewnętrznym dla rozwoju narodu i państwa. Do zbioru wartości chronionych należą m.in., jakość życia, niezależność polityczna, terytorialna integralność[2].

Rola państwa na płaszczyźnie zapewniania obrony narodowej w ówczesnych czasach skupia się na płaszczyźnie wojskowo-politycznej. Jednakże ciągle rozwijająca się cyfryzacja w obrębie, której nieustannie dokonuje się przemian technicznych, organizacyjnych, technologicznych, ekonomicznych, ekologicznych, kulturowych i społecznych, wymusiła poszerzenie o nowe płaszczyzny. Na przełomie XX i XXI w. wśród tych płaszczyzn, bezpieczeństwo informacyjne jak i bezpieczeństwo ekonomiczne zostało uznane za dziedzinę priorytetową bezpieczeństwa narodowego[3].

W erze globalizmu informacji, bezpieczeństwo systemu informacyjnego jest nieustannym obiektem skupiającym na sobie cyberataki, w związku z powyższym wymaga nie tylko odpowiedniego systemu zabezpieczeń poprzez ochronę prawna i system teleinformatyczny. Prawne uregulowania w połączeniu z właściwym systemem informacyjnym mają szansę ograniczyć zagrożenia występujące w strefie informacji do jak najbardziej akceptowanych.

Skuteczna, trwała ochrona systemu informacyjnego w dużym stopniu wymaga monitoringu otoczenia wewnętrznego i zewnętrznego w organizacji. Narastająca ilość przestępstw w obszarze informacji oraz w pewnych przypadkach bezradność wynikająca z trudności identyfikacji cyberprzestępców, stanowią o istocie podjętej problematyki. Można, zatem stwierdzić, iż jest zauważalny deficyt specjalistów zajmujących się ochroną systemów informacyjnych przed osobami nieuprawnionymi do ich posiadania tzw. hakerami.

Cyberprzestępcy, konkurencja rynkowa, kierują się chęcią osłabienia, zniszczenia a nawet przejęcia jednostek organizacyjnych, co jest szczególnie rażącym w skutkach zagrożeniem.

---

[1] PN-ISO/IEC 17799:2007, s. 9

[2] J. Janczak, A. Nowak, *Bezpieczeństwo informacyjne. Wybrane problemy, AON,* Warszawa 2013, s. 10-11.

[3] J. Janczak, A. Nowak, *Bezpieczeństwo…dz. cyt.*, s. 12.

W kulturze globalnej prawa i polityki wszystkie treści są informacją, a człowiek sam sprowadzany jest do obiektu w systemie teleinformatycznym. Przeniesienie informacji na drogę sieciową, cyfrową pozwala nad nimi zapanować, kontrolować i stymulować[1].

2.2. Znaczenie informacji, funkcje, narzędzia służące do jej oceny

Teraźniejsze czasy pokazują jak informacja zdominowała świat zarówno rzeczywisty jak i wirtualny. Globalizm poszerzył horyzonty w zakresie rozwoju cywilizacyjnego, gospodarczego w oparciu o implementację nowoczesnych technik i technologii, jednakże wraz z nim pojawiły się także zagrożenia dotyczące bezpieczeństwa systemów informacji. Zagrożona jest informatyzacja danych w związku z faktem, że jest ona powszechna, często w niewystarczający sposób zabezpieczona a użytkownicy bagatelizują zagrożenia wynikające z niewłaściwego użytkowania.

Uczelnia wyższa to organ publiczny, posiadający liczne, różnorodne zasoby informacji, wpływające z zewnątrz oraz wypływające na zewnątrz jak również przekazywane wewnątrz uczelni pomiędzy wszelkiego rodzaju działami, jednostkami. Droga przekazu wiadomości wynika ze struktury organizacyjnej jednostki. Słowo informacja pochodzi z języka łacińskiego, *informatio* oznaczając wizerunek, zarys, pojęcie, zaś czasownik *informo,* oznacza kształtowanie, tworzenie, wyobrażanie sobie, przedstawienie, opisywanie, kreślenie, kształcenie, uczenie[2]. Literatura przedmiotu pokazuje, ze informacja ma wiele definicji, a jej brzmienie jest uzależnione od różności dyscyplin naukowych. Jedną z nich jest np. rozumienie informacji, jako *nazwa treści zaczerpniętej ze świata zewnętrznego. Proces otrzymywania i wykorzystania posiadanej informacji jest procesem dostosowania się do różnego rodzaju ewentualności zewnętrznego środowiska oraz współistnienia w tym środowisku*[3].

W zasygnalizowanych obszarach pokolenia mogą się różnić od siebie a to może wynikać z podejścia odmiennego do samej definicji, jaką jest informacja oraz różnic w postrzeganiu przez badaczy rzeczywistości. Informacja to w jakimś sensie bodziec oddziaływujący na układ recepcyjny człowieka, który po przeistoczeniu powoduje wytwo-

[1] J. Janowski, *Cyberkultura prawa. Współczesne problemy filozofii i informatyki prawa*, Warszawa 2012; J. Janowski, Globalna cyberkultura polityki i prawa, http://www.bibliotekacyfrowa.pl/Content/46512/23_Jacek_Janowski.pdf, s. 316 i n. [dostęp: 24.10.22].
[2] *Słownik łacińsko-polski w opracowaniu Kazimierza Kumanieckiego*, PWN, Warszawa 1975, s. 260.
[3] S. Forlicz, *Informacje w biznesie*, PWE, Warszawa 2008, s. 13.

rzenie w wyobraźni przedmiotu myślowego mającego odzwierciedlić obraz rzeczy materialnej czy abstrakcyjnej (procesu, przedmiotu, zjawiska, pojęcia), mającej skojarzenie z tym bodźcem. Fakt ten oznacza, że informacje to są tylko te doznania, mające inspirować umysł ludzki do pewnej wyobraźni a jej istnienie jest relatywnie powiązane z istnieniem człowieka oraz jego umysłu (L. Ciborowski, 1990)[1].

Zauważalne są głosy, że informacja to wiedza niezbędna do określenia jak i realizacji zadań, służących do osiągnięcia celów w organizacji. Definicja ta jednoznacznie podkreśla czynnik wartości dla organizacji. Spotkać się można także z innymi definicjami, które głoszą, że informacja to właściwość sygnału lub wiadomości na zmniejszeniu nieokreśloności czy niepewności wynikającej ze stanu albo dalszego rozwoju sytuacji, której ta wiadomość dotyczy[2]. Należy również wspomnieć o ujęciu odróżniającym termin danych od pojęcia informacji szeroko rozumianej, jako dane już wcześniej przetworzone, mające nadane cechy charakterystyczne dla wartości jednostki, czyli wartość w procesie decyzyjnym[3]. Nie należy zapominać że informacja to czynnik, który zmniejsza skalę niewiedzy o konkretnym zjawisku i umożliwia podjęcie właściwej decyzji, sprawniejsze działanie[4].

W procesie decyzyjnym niekwestionowana rola informacji przybiera charakter strategiczny. Informacja jest źródłem wiedzy, a jej wykorzystanie daje władzę. Na optymalną decyzję jest szansa wtedy, jeżeli posiadana informacja jest wiarygodna, sprawdzona i jest jej dużo[5]. Informacja poddana analizie pozwala w dużym stopniu na wyselekcjonowanie informacji trwałej lub krótkotrwałej oraz wiarygodnej mającej miano dobrej lub niewiarygodnej o mianie złej[6]. M. Maciejewski przedstawia szeroką definicję informacji postrzegając ją, jako utrwalony w sposób dowolny, także w pamięci człowieka komunikat świadomości i wiedzy o jakimś konkretnym fakcie.

Komunikat może być utrwalony w sposób materialny, elektroniczny na nośniku danych, możliwy do odczytania przez inne osoby. Przy sposobie niematerialnym nie ma możliwości odczytania informacji przez inne osoby, ponieważ komunikat znajduje się

[1] R. Kwećka, *Informacja w walce zbrojnej,* AON, Warszawa 2001, s. 17.
[2] G. Gierszewska, M. Romanowska, *Analiza strategiczna przedsiębiorstwa*, PWN, Warszawa 1997, s. 21.
[3] K. Kolegowicz, *Informacja w zarządzaniu przedsiębiorstwem*, red. R. Borowiecki, M. Kwieciński, Kantor Wydawniczy Zakamycze, Kraków 2003, s. 54.
[4] M. Witkowska, K. Cholawo-Soszoch, *Społeczeństwo informacyjne. Istota, rozwój, wyzwania,* Wydawnictwo Akademickie i Profesjonalne, Warszawa 2006, s. 99
[5] P. Sienkiewicz, *Społeczeństwo informacyjne jako system cybernetyczny,* Uczelniane Wydawnictwo Naukowo-Dydaktyczne, Kraków 2004, s. 23.
[6] J. Wołejszo, *System dowodzenia,* AON, Warszawa 2013, s. 159.

w pamięci człowieka[1]. Definicja uniwersalna została przyjęta w ramach OAIS (Open Archival Information System) i wykorzystywana jest między innymi przez NASA. Według owej definicji informacja to wiedza w dowolnym ujęciu, dzieląca się niezależnie do formy fizycznej, cyfrowej, użytej dla jej wyrażania. Z kolei dane stanowią zgodne formy reprezentacji informacji. Dostęp do tych informacji jest dla osoby posiadającej konkretne dane[2]. Informację w PN-ISO/IEC 2383-16: 2000 *Technika informatyczna - Terminologia – Teoria informacji,* definiuje się, jako, wiedzę redukującą czy usuwającą niepewność dotyczącą konkretnego zdarzenia z konkretnego zbioru zdarzeń możliwych[3].

Krzysztof Liedel, pochylił się nad przeglądem definicji informacji opisanych przez różnych badaczy, według jego opinii dotykają jedynie wybranych aspektów a mianowicie:

- informacja to zbiór faktów, cech i zdarzeń, określonych obiektów, procesów, rzeczy, systemów, zawartych w wiadomości, przekazanym komunikacie, ujętych i podanych w formie pozwalającej odbiorcy ustosunkować się do zaistniałej sytuacji oraz podjąć odpowiednie działania fizyczne czy też umysłowe (Piotr Sienkiewicz);
- informacja to wiedza, która została wpojona, pozyskana na studiach przy obserwacjach czy badaniach naukowych, wchłaniana z otoczenia (Andrew Webster);
- informacja jest transformacją jednego komunikatu asocjacji informacyjnej w komunikat drugi tej asocjacji a informowanie jest to transformowanie informacji zawierających się w łańcuchu obrazów (Marian Mazur);
- informacja oznacza bodziec oddziałujący na układ recepcyjny człowieka, mający na celu wytworzenie w wyobraźni myślowego przedmiotu mającego swoje odzwierciedlenie w obrazie rzeczy materialnej bądź abstrakcyjnej, który w jego świadomości będzie się kojarzył z tym bodźcem. Oznacza to, iż informacja to nie jest tylko doznanie, inspirujące umysł ludzki do wyobraźni. Następuje tutaj relatywny związek informacji z istnieniem człowieka jak i jego umysłem (Leopold Ciborowski);
- informacja to czynnik sterujący strumieniami zasileń, znajdujący swoje wykorzystanie w maszynach lub organizmach żywych do bardziej efektywnego i sprawnego działania (Edward Kowalczyk);

[1] M. Maciejewski, *Prawo informacji – zagadnienia podstawowe, [w:] Prawo informacji. Prawo do informacji,* red. W. Góralczyk, Wydawnictwo Wyższej Szkoły Przedsiębiorczości i Zarządzania im. Leona Koźmińskiego, Warszawa 2006, s. 31.
[2] L. Reich, D. Sawyer, *Archiving Referencing Model,* White Book, Issue 5, CCSDS 19.
[3] F. Wołowski, J. Zawiła Niedźwiecki, *Bezpieczeństwo systemów informacyjnych. Praktyczny przewodnik zgodny z normami polskimi i międzynarodowymi*, Edu-Libri, Kraków-Warszawa 2012, s. 16.

- informacja to wiadomość uzyskana przez człowieka poprzez obserwację lub czynność umysłową, wykorzystywaną w przekazie, układzie nadawca-odbiorca (Henryk Greniewski),
- informacja jest nie tylko wiadomością o czymś, ale także każdą decyzją, poleceniem czy sugestią (Norbert Wiener).

Czesław Bierman, pojęcie informacji rozpatrywał w kategoriach takich jak: rzecz, potencjał, wielkość mierzalna, zmiana a informacje w sensie rzeczy zdefiniował, jako produkt określonego procesu posiadającego wykonawcę, źródło informacji oraz użytkownika, czyli odbiorcę. Informacja w rozumieniu, jako rzecz, może być wytwarzana, magazynowana, przesyłana (przekazywana), przetwarzana, sprzedawana. Określając informację można jej przypisać pewne właściwości, jakimi są treść, forma, wielkość, użyteczność, wartość. Informacja określana jest wielkością mierzalną m.in. mającą postać konkretnej liczby czy znaku. W przypadku rozpatrywania jej, jako potencjał, ma ona zdolność do zmiany określonego stanu rzeczy na skutek eliminacji lub zmniejszenia niepewności potencjalnego odbiorcy w odniesieniu do stanów przez niego rozważanych, wyboru z możliwych stanów[1].

Podsumowując rozważania na temat definicji informacji K. Liedel wnioskuje, że informacja może występować w systemie, jako sprawczy czynnik, w odniesieniu do zjawisk, nie występujących w obecnej chwili, które nie występowały w przeszłości jednakże pojawiają się w przyszłości. Informacja także może istnieć obiektywnie i nie jest zależna od świadomości oraz woli człowieka, dotyczyć może zjawisk i procesów nierealnych, które w danym procesie nie miały możliwości zaistnieć jak i nie zaistnieją w przyszłości. Może być ona przetwarzana, powielana, przekazywana w czasie oraz przestrzeni, z wyszczególnieniem technik informacyjno-telekomunikacyjnych.

W opinii K. Lidermana, informacja może być przenoszona w czasie, czyli magazynowana, zapamiętywana oraz przenoszona w przestrzeni za pomocą komunikacji i transmisji. Przenoszenie, przekazywanie informacji najczęściej odbywa się za pośrednictwem nośników informacji z wykorzystaniem zjawisk fizycznych. Magazynowanie jest wyrażone za pomocą obiektu fizycznego np. zapisu a transmisja za pomocą określonego zjawiska fizycznego np. sygnału[2]. Zbiór informacji należy do zbioru niewyczerpanego, czyli informacja w przeciwieństwie do innych zasobów nie zużywa się w procesie

[1] K. Liedel, *Zarządzanie informacją w walce z terroryzmem,* Wydawnictwo TRIO, Warszawa 2010, s. 42-45.
[2] K. Liderman, *Bezpieczeństwo informacyjne,* PWN, Warszawa 2012, s. 17.

jej wykorzystania. Podstawową cechą informacji jest jej różnorodność, mogą one podlegać deformacji, wszelkiego rodzaju przekształceniu, zafałszowaniu na skutek nieświadomego lub świadomego działania człowieka czy chociażby zdarzeń losowych, przypadkowych. Cechą specyficzną informacji jest konieczność jej bieżącego aktualizowania. Informacja także musi być wyrażona jasnym komunikatem za pośrednictwem nośnika[1].

Różne postrzeganie w literaturze pojęcia odnoszącego się do informacji może mieć wpływ na pogląd systemów informacyjnych, które oddziałują na podstawową strukturę oraz schemat organizacji wprowadzając poprawę skuteczności i sprawności działania jednostek.

Informacja, na której oparty jest rozwój cywilizacji według K. Lidermana to:

- dla państwa, organizacji, człowieka, informacja jest *towarem często o znaczeniu strategicznym;*
- przerwanie obiegu informacji bądź jej sfałszowanie powoduje straty dla podmiotów, zaś dla państwa wywołuje niepokój społeczny, zaburzenia w gospodarce i na forum międzynarodowym gorsze jej postrzeganie. Dlatego informacja jest *podstawowym elementem procesów biznesowych;*
- informacja może występować w postaci informacji sterującej urządzeniami, czujnikami, wykonawczymi mechanizmami. W związku z powyższym sterowanie takimi systemami może wywołać kryzys w skali lokalnej, ogólnokrajowej, międzynarodowej jak i powodować katastrofy. Dlatego też, informacja *służy do sterowania procesami w zautomatyzowanych procesach wytwórczych i usługowych o kluczowym znaczeniu dla społeczeństwa i gospodarki;*
- *jest chroniona na mocy obowiązującego prawa jak i zawartych umów*, dotyczy wszystkich krajów cywilizowanych wymuszając ochronę informacji przed dostępem do niej osób nieuprawnionych mających złe intencje, zapewniając jej prawidłowe przetwarzanie, przechowywanie, przesyłanie[2].

Strategiczne znaczenie informacji, funkcje:

- *funkcja modelowania,* w tym przypadku informacja stanowi obraz rzeczywistości będący miarą różnorodności, złożoności, badanego wycinka rzeczywistości,
- *funkcja sterująca,* zastosowana w różnych bazach danych i wiedzy, stanowiących podstawę planowania oraz podejmowania decyzji,

[1] K. Liedel, *Zarządzanie informacją w walce…dz. cyt.*, s. 45.
[2] K. Liderman, *Bezpieczeństwo…dz. cyt.*, s. 15.

- *funkcja decyzyjna,* informacja jako motywator do działania i osiągania celów,
- *funkcja kapitałotwórcza,* ziemia kapitał, praca,
- *funkcja rozwoju wiedzy,* cywilizacyjna,
- *funkcja konsumpcyjna,* jej założenie zakłada, że informacja traktowana jest, jako towar[1],
- *funkcja kulturotwórcza*[2]*,* jest ostatnią funkcją, o jakiej należy wspomnieć w celu przybliżenia istoty pojęcia informacji.

Istnieje jeszcze podział na informacje wrażliwe i niewrażliwe. Informacje wrażliwe w odniesieniu do konkretnego podmiotu charakteryzują się tym, iż mogą być wykorzystane poprzez ich ujawnienie, udostępnienie i zmanipulowanie, przeciwko jego interesom[3]. Do informacji wrażliwych zgodnie z obowiązującym prawem zaliczyć należy, wszystkie informacje, które z różnych względów powinny być chronione, nieupublicznione, nieprzekazywane osobom postronnym[4].

Do takich informacji zaliczyć można również informacje, których nakaz ochrony nie ma umocowania w żadnych regulacjach prawnych jednakże mają wskazanie kompetentnych do tego organów, czyli wewnętrzne komórki bezpieczeństwa, służby ochrony państwa itp.. Takimi informacjami mogą być też dane, które same w sobie nie mają miana niewrażliwych jednakże w połączeniu z innymi informacjami już można wyciągnąć konkretne wnioski np. informacje strategiczne firmy.

Najczęściej identyfikacja informacji wrażliwej w organizacji ogranicza się do jej starannej inwentaryzacji, przeglądu zasobów w ramach analizy ryzyka. Jednakże powinny być one również zlokalizowane poza organizacją ze ścisłym uwzględnieniem informacji pośrednich pozwalających na wnioskowanie. Zidentyfikowanie także obiegu informacji wrażliwej pozwala na np. opracowanie procedury lokalizacji jej przenikania. Dodatkowo sprawa dotycząca informacji komplikuje się w przypadku, kiedy prawo własności jest często trudne do określenia czy lokalizacja informacji wartościowych bywa

[1] K. Liedel, T. Serafin, *Otwarte źródła informacji w działalności wywiadowczej,* Difin, Warszawa 2011, s. 38.
[2] K. Liedel, *Zarządzanie informacją w walce…dz. cyt.,* s. 45.
[3] Należy zwrócić uwagę, że wprowadzone określenie informacje wrażliwe ma szerszy zakres niż takie samo określenie stosowane zwyczajowo do informacji wymienionych w art. 27 *Ustawy o ochronie danych osobowych i o których w tym samym kontekście mówi p. 51 Rozporządzenia UE*.
[4] Ustawa o ochronie danych osobowych, *Ustawa o ochronie informacji niejawnych* oraz przepisy, w których zdefiniowano tzw. tajemnice, np. tajemnicę przedsiębiorstwa.

trudna. Na podstawie zgromadzonych informacji można podsumować, iż osoby odpowiedzialne za ochronę informacji powinny przestrzegać zasad, dbać o ochronę informacji. Nie odpowiednie podejście do ochrony informacji jest błędem organizacyjnym.

Przyjmuje się, że informacje, jako przedmiot przetwarzania w systemach informatycznych nazywa się danymi a specjaliści techniki komputerowej to właśnie takim pojęciem się posługują[1]. Według E. Mistewicza wystąpił „ attention crash", czyli ilość informacji, jaką każdy człowiek chciałby przyswoić zdecydowanie przekracza jego zdolność uwagi, co świadczy o tym ze percepcja odbiorcy informacji zostaje zablokowana. Obecnie ilość nowych informacji wzrasta, często są to informacje, które nie znajdują potwierdzenia, nie są w pełni wartościowe. Mogą być spowodowane m.in. szumami w komunikacji. Natłok informacji przekazywanych często może powodować wydłużenie procesu decyzyjnego oraz zwiększa ryzyko niewłaściwego sposobu odbioru informacji, co w ostateczności zaburza sprawne, zarządzanie jednostką organizacyjną. W podmiotach gospodarczych gromadzone są duże ilości danych, zapełniają one serwery oraz archiwa[2]. Przesycenie informacją wymaga jej weryfikacji pod dwoma względami, jakościowym i ilościowym.

Siedemnaście narzędzi, które można wykorzystać do oceny, jakości informacji:

- *aktualność,* informacja ma miano zmiennej bez opóźnień odpowiednio do zmian przedmiotu opisu;
- *dokładność,* informacja jest precyzyjna i zaprezentowana w sposób odpowiedni do poziomu wiedzy jej użytkowników;
- *kompleksowość,* informacja jest dostępna w ilości i stopniu szczegółowości zgodnym z wymaganiami jej użytkowników;
- *relewantność,* określa czy dana informacja jest istotna dla odbiorcy i związana z tym, co jest poszukiwane przez odbiorcę;
- *spójność,* poszczególne fragmenty informacji nie są sprzeczne, są przekazywane i prezentowane w jednolitej formie oraz dotyczą zadanego tematu,;
- *odpowiedniość formy,* informacja jest prezentowana w takiej formie, która minimalizuje jej błędną interpretację;

[1] K. Liderman, *Bezpieczeństwo…dz. cyt.,*, s. 17-18.
[2] M. Karnowski, E. Mistewicz, *Anatomia władzy*, Wydawnictwo Czerwone i Czarne, Warszawa 2010, s.138-139.

- *wiarygodność,* informacja zawiera elementy, które mogą upewnić odbiorcę o rzetelności przekazu[1];
- *celowość,* zdolność, jaką informacja posiada do wyznaczania norm w procesie sterowania;
- *agregację,* poziom syntezy informacji;
- *komunikatywność,* mierzona niezbędna ilość pracy dla nadania przez odbiorcę jej formy dopuszczającej wnioskowanie i podjęcie decyzji;
- *jednoznaczność,* określenie jednoznaczne języka i precyzyjnie określonych pojęć;
- *wartość,* sprawienie zmiany wartości decyzyjnej sytuacji;
- *porównywalność*, porównanie informacji z informacjami innymi;
- *decyzyjność,* stopień spływu na proces decyzyjny;
- *prawdziwość,* opisywana rzeczywistość jest zgodna z treścią informacji;
- *wierność,* informacja w zbiorze oryginałów jest taka sama co w zbiorze obrazów;
- *źródłowość*, pochodzenie z obserwacji informacji bezpośredniej czy pośredniej[2].

Przy potocznej analizie oraz ocenie, jakości przekazu informacyjnego można zauważyć, że kryteria dotyczą jednakże samej treści, formy i użytkownika. Jednakże przy ocenie, jakości informacji nie jest to wystarczające pod względem cyberprzestrzeni. W związku z powyższym wymaga ona jeszcze dodatkowego narzędzia, jakim jest informacja ją opisująca, czyli tak zwany kontroler dla posiadanych danych, innymi słowy kody detekcyjno-korekcyjne, cyfrowy podpis.

Do przykładowych informacji opisujących umieszczanych na stronach Internetowych są m.in.:

- *informacje uwierzytelniające prezentowane treści (ang. authority)* – z wykorzystaniem źródeł informacji, danych i rekomendacji dotyczących podmiotów opracowujących treści oraz daty dostarczenia;
- *informacje o interesariuszach (ang. transparency and honesty)* – zawiera dane identyfikacyjne administratorów strony, dostawców treści, sponsorów czy reklamodawców, określeniu również podlegają zamiary i cele właściciela strony internetowej jak i docelowej grupy, do której zamieszczony jest konkretny przekaz (informacja);
- *informacje o aktualności treści (ang. updating of information)* – wprowadzone uaktualnienia linków i dat zmian;

[1] K. Liderman, *Bezpieczeństwo…dz. cyt.*, s. 16.
[2] K. Liedel, *Zarządzanie informacją w walce…dz. cyt.*, s. 48-49.

- *informacje o stosowanej polityce zachowania prywatności i ochrony danych (ang. privacy and data protection)* – wskazanie zgodności z obowiązującymi przepisami prawa, polityki prywatności oraz polityki zabezpieczenia własności intelektualnej;
- *informacje umożliwiające rozliczalność (ang*. accountability) – dane kontaktowe, identyfikacyjne osób przygotowujące pod względem merytorycznym treść strony www oraz zasady edytowania stron czy doboru materiału[1].

W odniesieniu do technicznego aspektu strony przetwarzania informacji należy w tym miejscu wyróżnić 6 kryteriów, jakości, ściśle związanych z ochroną informacji:

- *tajność* – przetwarzane informacje mające wymagany stopień ochrony przed nieuprawnionym dostępem do nich osób trzecich. Stopień tajności zasugerowany przez osoby czy organizacje otrzymujące i dostarczające te informacje;
- *dostępność* – oznacza wymagany przez użytkownika stopień dostępności danych procesów i aplikacji;
- *integralność* – oznacza, iż na informacji nie zostały w żaden sposób wykonane niedozwolone działania;
- *rozliczalność* – istnieje możliwość identyfikacji użytkowników, systemu teleinformatycznego, oraz wykorzystanych przez nich usług. Dzięki temu kryterium rozliczeniowości jest możliwość prowadzenia skutecznej analizy na skutek włamania;
- *autentyczność* – jest to jednoznaczna możliwość identyfikacji, jaki podmiot przesłał dane;
- *niezaprzeczalność* – informacje o możliwości wyparcia się uczestnictwa przez przedmiot uczestniczący w wymianie informacji.

Na dobór wymienionych powyżej kryteriów, jakości informacji wpływa polityka przedmiotu jak i przyjęte rozwiązania organizacyjne, techniczne, systemu w jakim są one przetwarzane[2].

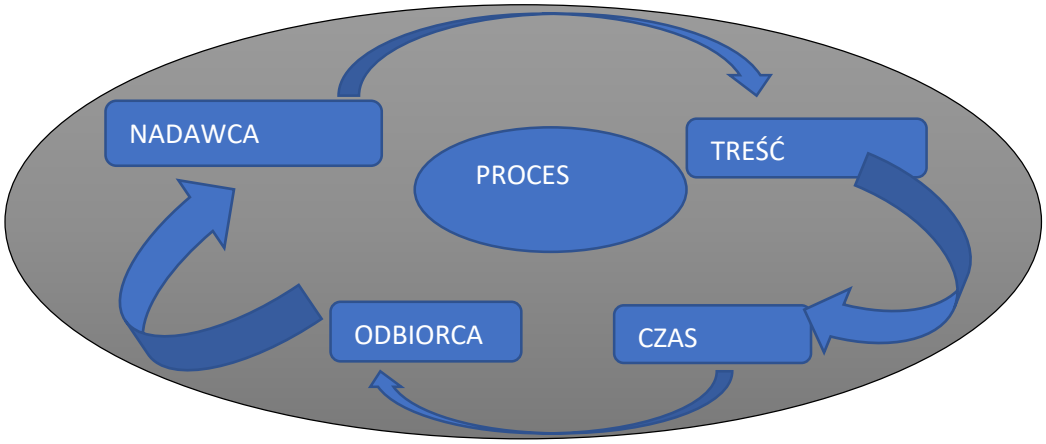
Techniczny aspekt oceny informacji pozwala organizacji ocenić jej istotność w ochronie przekazu zwracając uwagę na identyfikację samego nadawcy czy weryfikację użytkowników, mając gwarancję jej dostarczenia do odpowiedniego odbiorcy. Często zdąża się, że informacja została przesłana jednakże odbiorca zaprzecza jakoby ją otrzymał. Podważany fakt przesłania informacji rodzi kontrowersje z uwagi na jednostkę

[1] K. Liderman, *Bezpieczeństwo…dz. cyt.,* s. 16.
[2] Tamże, s. 17.

czasu, która w sprawach niecierpiących zwłoki nabiera znaczenia strategicznego. Na rysunku 2.1 został przedstawiony uproszczony proces obiegu informacji.

Uznanie informacji za kluczowy element przewagi stanowi nieodłączną cechę współczesnych konfliktów, w których informacja jest wykorzystywana na różnych płaszczyznach np., jako broń, cel. Teoretycy wskazują na konieczność traktowania sfery informacyjnej, jako nowoczesnego środka walki[1]. W czasach współczesnych w połączeniu z nowymi technologiami informacyjnymi oraz komunikacyjnymi, człowiek jest w jakimś sensie uzależniony od podręcznych nośników[2].

Rysunek 2.1. **Proces obiegu informacji**



Źródło: Opracowanie własne

Studium przypadku

Konferencja bliskowschodnia w pełni obrazuje potęgę militarną informacji dla służb wywiadowczych. Spotkanie ministerialne zostało zaplanowane w Warszawie i przypadało na 13-14 lutego 2019 r.. Było poświęcone budowaniu pokoju i bezpieczeństwa na Bliskim Wschodzie. W tym czasie była ona najważniejszym wydarzeniem dyplomatycznym w Warszawie od czasu szczytu w NATO.

Współgospodarzami były Polska i Stany Zjednoczone a udział w niej wzięły kraje z całego świata, które były zainteresowane rozwojem sytuacji, jaka miała miejsce na Bliskim wschodzie. Spotkanie to stanowiło cel dla terrorystów i cyberprzestępców.

[1] B. Balcerowicz, *Siły zbrojne w stanie pokoju, kryzysu i wojny*, Wydawnictwo Naukowe Scholar, Warszawa 2010, s. 218.
[2] M. Majchrzak, *Wpływ rozwiązań informacyjnych na funkcjonowanie społeczeństwa, „Studia Kaliskie"*, t. 7, 2019, s. 91.

Świadomość zagrożenia i sprzeciw strony irańskiej na organizacje tej konferencji w Warszawie spowodował, iż służby zwiększyły działania prewencyjne w ochronie m.in. informacji, osób i mienia. Obecny premier Mateusz Morawiecki w ramach zwiększenia bezpieczeństwa na terenie Warszawy wprowadził stopień alarmowy ALFA od dnia 11-15.02.2019 r.. Stopień ten jest najniższym stopniem alarmowym w czterostopniowej skali i określony w ustawie antyterrorystycznej. Jego przełożenie na funkcjonowanie w tych dniach obywateli zamieszkujących Warszawę oraz przyjezdnych osób związane było z wzmożoną kontrolą pojazdów, stacji metra, skupisk ludzi a nawet miejsc użyteczności publicznej. Współczesne praktyki, co do informacji są bardzo złożone i trudne w ich wyjawianiu ponieważ w cyberprzestrzeni jest duża anonimowość.

Poszukiwanie nowych rozwiązań innowacyjnych, technicznych, technologicznych emituje nowe zagrożenia dla informacji o znaczeniu, gospodarczym, politycznym, militarnym. Służby nieustanie informują o zorganizowanych działaniach o charakterze przestępczym polegającym na przechwyceniu zasobów informacji i tym przykładem może być Firma Huawei.

Ważną kwestią są naruszenia związane z dużym zaniedbaniem. Firmy, u których w 2022 roku wykryto niepoprawne funkcjonowanie to m.in. Santander Bank Polska. Bank ten powiadomił klientów o naruszeniu danych. Wyciek danych polegał na tym, że pracownik mimo zakończenia pracy w tej instytucji w dalszym ciągu miał dostęp do profilu płatnika na Platformie Usług Elektronicznych ZUS.

Kolejnym przypadkiem, o którym warto wspomnieć jest Spółka Fortum Marketing and Sales Polska, we wspomnianej spółce nie zostały wprowadzone odpowiednie zabezpieczenia a co za tym idzie brakowało weryfikacji podmiotu przetwarzającego. W tym przypadku proceder polegał na skopiowaniu danych klientów przez osoby do tego nieuprawnione.

Następny przypadek, który warto poruszyć to Główny Geodeta Kraju, a sprawa dotyczyła pojawienia się w serwisie geoportal.gov.pl numerów ksiąg wieczystych obywateli i taka informacja na temat danych widniała na tej stronie ok 48 h[1].

Rywalizacja w dziedzinie produkcji mobilnych urządzeń nowej generacji Internetu stała się dla USA i Chin zagadnieniem bezpieczeństwa narodowego. Władze amerykańskie wprowadziły zakaz stosowania urządzeń produkcji Huawei przez rząd fede-

[1] https://www.money.pl/ gospodarka/firmy-i-instytucje-placa-kary-za-wycieki-danych-jakie-to-kwoty-mamy-dane-6862541067500128a.html [dostęp: 4.11.2022].

ralny w amerykańskich sieciach telekomunikacyjnych. Argumentacją powyższego zdarzenia było to, że urządzenia tej firmy uniemożliwiają chińskim szpiegom penetrację systemów w celu zdobycia tajemnic technologicznych. Waszyngton zabiega, aby wszyscy sojusznicy USA wprowadzili podobne zakazy stosowania produktów właśnie tej firmy[1].

B. Bryson w swojej książce *W domu* wskazał na fakt, że masowo zawłaszczano informacje, których pozyskanie dla wielu miało kluczowe znaczenie, aby osiągnąć sukces i zdobyć nie osiągalny do chwili obecnej cel. T. Edison, najwybitniejszy amerykański wynalazca poszukiwał tajnej metody oświetleniowej i bez zastanowienia oraz widocznej skrupuły kradł patenty, oszukiwał, zaś dziennikarzom płacił za to, aby o jego osobie dobrze pisali[2]. Takie działania są praktykowane we wszystkich obszarach związanych z działalnością człowieka. Informacja, która dla jednego będzie zasobem to dla przestępcy już będzie celem. W związku z tak szybkim rozwojem technologicznym eskalują także zagrożenia krążące wokół informacji która znacznie przybrała na sile. Sytuacja taka wskazuje na konieczność zadbania o bezpieczeństwo informacyjne.

2.3. Znaczenie bezpieczeństwa systemu informacyjnego

Amerykański psycholog A. Maslow w zaprezentowanej hierarchii potrzeb, potrzebę bezpieczeństwa umieścił wskazując od samego dołu, jako drugą zaraz po zaspokojeniu potrzeb fizjologicznych. Potrzeba bezpieczeństwa przejawia się w swojej postaci społecznej i międzyludzkiej stanowiąc podstawę każdej organizacji, funkcjonowania w życiu społecznym, państwowym, przy wykonywaniu codziennych czynności oraz w otoczeniu uczelnianym[3].

Postrzeganie bezpieczeństwa przez pryzmat konkretnej jednostki ma ścisły związek z realizacją podstawowej potrzeby rzędu niższego, jaka została w hierarchii potrzeb przez Maslowa wskazana. Bezpieczeństwo przyrównane może być np. do pewnego rodzaju granicy czy muru. Jest to w jakimś sensie odgrodzenie od potencjalnych niebezpieczeństw pochodzących z otaczającej nas rzeczywistości świata zewnętrznego. Taka granica czy mur dają poczucie *normalności* oraz *stabilizacji*, odczucia te zostały zbudowane wokół pozycji zawodowej, rodzinnej czy społecznej.

[1] http://wgospodarce.pl/informacje/57379-rozkreca-sie-afera-z-huawei [dostęp: 05.11.2022].
[2] B. Bryson, *W domu*, Wydawnictwo Zysk i S-ka, Poznań 2010, s. 150.
[3] P. Kotler, *Marketing*, REBIS, Poznań 2005, s. 662.

Niemiecki filozof, socjolog, psycholog E. From określił formy bezpieczeństwa powyżej wymienione, jako miano fiksacji, na których fundamentach opiera się społeczeństwo[1]. W literaturze przedmiotu mamy styczność z wieloma definicjami bezpieczeństwa, a są one uwarunkowane poglądowością ich autorów jak również dziedziną nauki, jaką reprezentują.

Przykładem może być R. Zięba, dokonał on podziału bezpieczeństwa na bezpieczeństwo wewnętrzne oznaczające stabilność i harmonijność organizmu, podmiotu oraz bezpieczeństwo zewnętrzne gdzie występuje brak zagrożenia ze strony innych czynników i podmiotów zewnętrznych[2]. Jego teza bezpieczeństwa określona jest, jako pewność istnienia oraz przetwarzania, posiadania, funkcjonowania i rozwoju podmiotu. Pewność powstaje w skutek kreatywnej działalności danego podmiotu, jest zmienną w czasie, czyli ma naturę procesu społecznego, nie jest wynikiem tylko braku zagrożenia[3].

Słownikowa forma określenia bezpieczeństwa to stan *niezagrożenia*[4], w którym jednostka ma poczucie spokoju, pewności, odczuwa zadowolenie i oparcie w osobie drugiej czy nawet sprawnie działającym systemie prawnym. Analizując tą definicję można zauważyć, iż bezpieczeństwo jest przeciwieństwem zagrożenia[5]. K. Liedel pojęcie bezpieczeństwa określił, jako stan rzeczy, ciągły proces społeczny, w którego ramach działające podmioty starają się doskonalić mechanizmy zapewniające właśnie poczucie bezpieczeństwa[6]. T. Łoś-Nowak uznaje, że to pojęcie jest trudne do zdefiniowania. Bezpieczeństwo to nie tylko w gruncie rzeczy stan możliwy do określenia jedynie w ustalonym miejscu, czasie, czyli *tu i teraz (hic et nunc),* ale także dynamiczny proces ciągle się zmieniający w czasie[7]. J. Piowowarski zauważa, że bezpieczeństwo w ujęciu dynamicznym stanowi proces społeczny, polegający na prowadzeniu przez podmiot bezpieczeństwa

[1] E. Fromm, *Ucieczka od wolności,* Czytelnik, 1978, s. 7.
[2] R. Zięba, *Instytucjonalizacja bezpieczeństwa europejskiego,* Wydawnictwo Scholar, Warszawa 1999, s. 27.
[3] R. Zięba, *Bezpieczeństwo międzynarodowe po zimnej wojnie,* Wydawnictwa Akademickie i Profesjonalne, Warszawa 2008, s. 16.
[4] *Słownik języka polskiego*, PWN, Warszawa 1979, s. 147.
[5] *Słownik współczesnego języka polskiego*, Wydawnictwo Wilga, Warszawa 1996, s. 50.
[6] K. Liedel, *Bezpieczeństwo informacyjne w dobie terrorystycznych i innych zagrożeń bezpieczeństwa narodowego*, Wydawnictwo Adam Marszałek, Toruń 2005, s. 8.
[7] T. Łoś-Nowak, *Bezpieczeństwo, [w:] Leksykon politologii*, red. A. Antoszewski, R. Herbut, Alta 2, Wrocław 2003, s. 37-38.

działań ciągłych mających podążać do doskonalenia mechanizmów kultury bezpieczeństwa, mających zapewnić temu podmiotowi istniejący i optymalny poziom w zakresie braku bądź redukcji zagrożeń dla jego bezpieczeństwa[1].

Podsumowując rozważania należy stwierdzić, że bezpieczeństwo to gwarant stabilności każdej jednostki ludzkiej i każdego podmiotu, aczkolwiek należy zaznaczyć, iż jego utrzymanie wymaga stałej kontroli i odpowiedniego zabezpieczenia przed napływającymi zagrożeniami.

Źródłem wszelkich zagrożeń mogą być umyślne i nieumyślne działania dokonywane na zewnątrz i wewnątrz organizacji.

Bezpieczeństwo każdej jednostki zależy od grup czynników takich jak:

- otoczenie bliższe,
- otoczenie dalsze,
- wewnętrzne poczucie bezpieczeństwa[2].

Każdy obywatel funkcjonuje w zmiennym otoczeniu, posiadającym następujące właściwości:

- *wzrost intensywności otoczenia* – oznacza wpływ elementów znajdujących się w otoczeniu na funkcjonujące w nim organizacje oraz wszystko, co jest z tym ściśle powiązane, czyli także ludzi;
- *szybkie tempo zmian zachodzących w otoczeniu* – skrócenie czasu na wprowadzenie zmian;
- *coraz większa liczba nowych nieznanych zmian* – w otoczeniu, w którym funkcjonuje człowiek występuje coraz więcej nowszych, niespotykanych zmian względem, których nie zostały wprowadzone rozwiązania i zgromadzone doświadczenia;
- *złożoność otoczenia* – wskazuje na zwiększenie liczby różnych elementów funkcjonujących w otoczeniu. Bardzo szybkie tempo przyrostu powoduje, że wpływ na bezpieczeństwo tych elementów staje się trudne do przewidzenia[3].

[1] J. Piwowarski, *Transdyscyplinarna istota kultury bezpieczeństwa narodowego*, Wydawnictwo Naukowe Akademii Pomorskiej, Słupsk 2016, s. 332–334.
[2] A. Rychły-Lipińska, *Model bezpieczeństwa jednostki we współczesnym zmieniającym się otoczeniu – wstępne rozważania,* „Studia nad bezpieczeństwem", nr 2, 2017, s. 37-38, http://cejsh.icm.edu.pl/cejsh/element/bwmeta1.element.desklightb3be4d04-9cf4-4281-9a41-1e502805c885 [dostęp: 12.10.2022].
[3] A. Rychły-Lipińska, *Model bezpieczeństwa jednostki we współczesnym zmieniającym się otoczeniu – wstępne rozważania,* „Studia nad bezpieczeństwem", nr 2, 2017, s. 42, http://cejsh.icm.edu.pl/cejsh/element/bwmeta1.element.desklightb3be4d04-9cf4-4281-9a41-1e502805c885 [dostęp:12.10.2022].

Reasumując bezpieczeństwo organizacji wymaga stałego rozpoznania środowiska w celu weryfikacji zagrożeń. Mogą one dotyczyć wszystkich jej sfer działalności a w szczególności tych pojawiających się w obrębie przekazu informacyjnego. Po podsumowaniu stwierdzeń badaczy na temat bezpieczeństwa jawi się wśród nich pełna zgodność. Informacja odgrywa kluczową rolę w dobie obecnego świata, opartego na cyfryzacji, rozwoju teleinformatycznym, co w większym stopniu potęguje zagrożenie jej bezpieczeństwa. Odwołując się do PN-ISO/IEC 17799: 2007 bezpieczeństwo informacji jest definiowane, jako ochrona informacji przed zagrożeniami a celem jest zapewnienie ciągłości działań, minimalizacji ryzyka, niepowodzenia i maksymalizacji zwrotu z inwestycji[1].

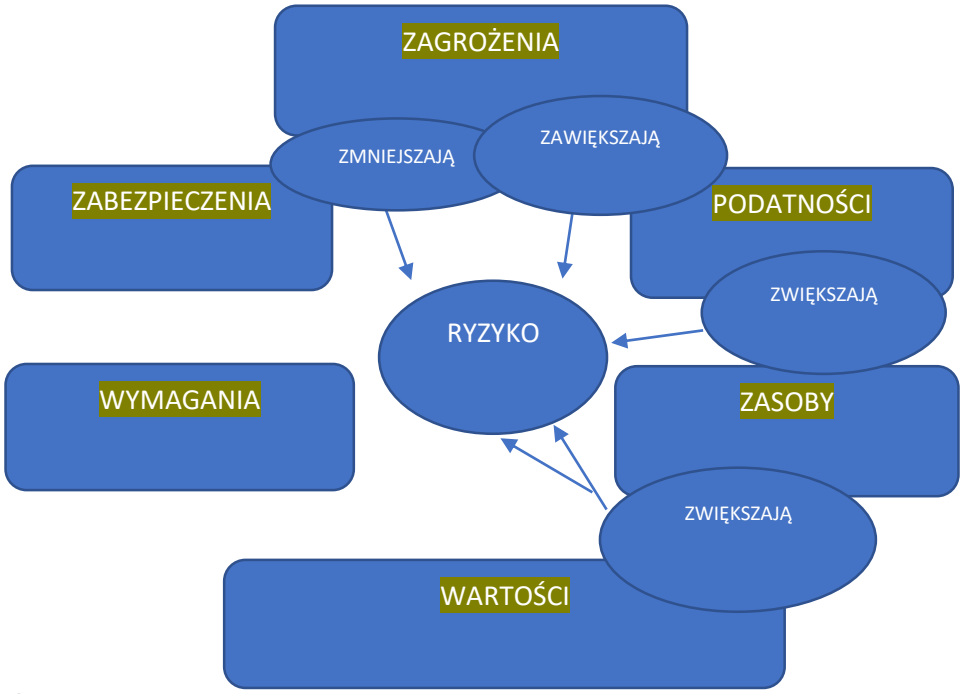
W normie PN-ISO/IEC 27001: 2017-06 *Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji* – Wymagania ISO pojęcie bezpieczeństwa informacji określane jest, jako zachowanie dostępności informacji, poufności, integralności.

Pod uwagę mogą być także brane inne własności np. niezaprzeczalność, niezawodność i autentyczność[2]. Wytyczne OECD odnoszące się do bezpieczeństwa informacji podają, że uzależnienie uczestników od systemów informatycznych, sieci wzrasta a w związku z tym od wszystkich tych elementów wymagana jest niezawodność oraz bezpieczeństwo. Skuteczny poziom bezpieczeństwa może być zapewniony w przypadku zapewnienia takiego podejścia, które będzie brało pod uwagę potrzeby wszystkich użytkowników, sieci i usług pochodnych oraz istoty systemów[3]. Na rysunku 2.2 przedstawione są relacje miedzy elementami bezpieczeństwa. Normy mające odniesienie do zarządzania bezpieczeństwem informacji wprowadziły sposób nadawania odrębnych nazw naukowych w celu ustandaryzowania nazewnictwa elementów bezpieczeństwa i ich wzajemnych interakcji[4]. Polska norma pokazuje, że bezpieczeństwo informacji stanowi o równowadze organizacji oraz możliwościach jej rozwoju w wolnym od zagrożeń otocze-

[1] PN-ISO/IEC 17799: 2007, Technika informatyczna - Technika bezpieczeństwa – Praktyczne zasady zarządzania bezpieczeństwem informacji, PKN, Warszawa 2007, s. 9.
[2] PN-ISO/IEC 27001:2017-06, s. 9.
[3] Overview OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security Polish translation, 2003, s. 3.
[4] J. Janczak, A. Nowak, *Bezpieczeństwo informacyjne…dz. cyt.*, s. 18-19.

niu, gdzie ochrona informacji jest pełna. Zdefiniowane relacje zachodzące pomiędzy elementami bezpieczeństwa, wskazują na potrzebę intensyfikacji działań zachodzących w obszarze ochrony zasobów.

Rysunek 2.2. Relacje pomiędzy elementami bezpieczeństwa



Źródło: opracowanie własne na podstawie normy: PN-I-13335-1: 1999, Wytyczne do zarządzania bezpieczeństwem systemów informatycznych, PKN, Warszawa 1999, s. 19.

Skuteczność wynika z prawidłowości systemu zabezpieczeń. Działania te podwyższają stan bezpieczeństwa informacji a co za tym idzie minimalizują ryzyko zagrożeń. Ochrona danych będących w posiadaniu jednostki to definicja odnosząca się do bezpieczeństwa informacji. Bezpieczeństwo informacji rozpatrywane w kontekście stopnia tajności informacji, sprawdzenia działań niedozwolonych poprzez identyfikację i nadanie użytkownikom uprawnień w myśl rozpatrywanej Polskiej Normy zabezpieczenia informacji przed zagrożeniami.

Według tezy K. Lidermana bezpieczeństwo informacji to uzasadnione zaufanie, brak poniesionych strat wynikających z niepożądanej zmiany, na skutek realizacji zagrożenia, istotnych kryteriów, jakości informacji oraz wymaganych wartości. Stwierdza również, że bezpieczeństwo informacji jest składową bezpieczeństwa informacyjnego. Należy trzymać się pewnego procesu a zatem najpierw taką informacje należy pozyskać,

przechowywać, przetwarzać, przesyłać a w między czasie w trakcie jej wykorzystania chronić[1].

Rozległość literatury pokazuje, że często dochodzi do przyrównywania bezpieczeństwa informacyjnego do bezpieczeństwa informacji. L.F. Korzeniowski w swojej książce zaznacza, że bezpieczeństwo informacyjne podmiotu, organizacji lub człowieka rozumiane jest, jako możliwość pozyskania dobrej, jakości informacji oraz jej ochrony przed utratą[2].

Powyższe stanowisko przyjmuje także K.Liderman, badacz problematyki bezpieczeństwa informacyjnego, dodaje jednocześnie, że w jego ocenia bezpieczeństwo informacyjne oznacza uzasadnione zaufanie podmiotu odnoszące się do dostępności i jakości pozyskiwanej oraz wykorzystanej informacji[3].

Dzięki tak rozległej analizie na temat bezpieczeństwa informacyjnego można wyciągnąć wnioski i określić, iż bezpieczeństwo informacyjne dotyczy:

- *systemów,* w których informacja jest wytworzona, przetworzona, przechowywana, przekazywana;
- *informacji,* jej specyficznej postaci, bardzo często nie jest ona uchwytna dla wielu osób (w bardzo łatwy sposób można zostać okradzionym);
- *personelu,* pracownicy organizacji często korzystają z tych systemów, jednakże zdarza się i tak, że personel jest nieprzeszkolony w odpowiedni sposób lub pewne działania wykonuje niedbale;
- *środowiska,* w którym systemy działają. Bardzo ważny jest każdy szczegół typu pomieszczenia, zasilanie;
- *całego otoczenia prawnego* dopiero się kształtującego.

Niejednokrotnie bezpieczeństwo informacyjne uznawane jest za element systemu informatycznego, jako zamiennik bezpieczeństwa telekomunikacyjnego, komputerowego[4], czy nawet bezpieczeństwa sieciowego[5].

Bezpieczeństwem informacyjnym, S. Kowalkowski, określa zakres bezpieczeństwa przyjmujący wzrost znaczenia informacji w zachowaniu stabilności międzynarodowych współczesnych systemów ekonomicznych i uwzględniający zabezpieczenie przed

[1] J. Janczak, A. Nowak, *Bezpieczeństwo informacyjne…dz. cyt.*, s. 22.
[2] L. F. Korzeniowski, *Podstawy nauk o bezpieczeństwie,* Warszawa 2012, s. 147
[3] K. Liderman, *Bezpieczeństwo informacyjne*…dz. cyt., s. 22.
[4] R. J. Sutton, *Bezpieczeństwo telekomunikacji,* przeł. G. Stawikowski, Wydawnictwo Komunikacji i Łączności, Warszawa 2004, s. 17.
[5] A. Nowak, W. Scheffs, *Zarządzanie bezpieczeństwem informacyjnym,* AON, Warszawa 2010, s. 22.

sieciowymi atakami, jak również skutkami ataków fizycznych i plasuje obok bezpieczeństwa ekonomicznego, politycznego, militarnego, społecznego, kulturowego, ideologicznego i ekologicznego[1].

Bezpieczeństwo informacyjne według E. Nowak i M. Nowak określone jest, jako stan warunków wewnętrznych i zewnętrznych dopuszczających do tego, aby państwo swobodnie rozwijało swoje społeczeństwo informacyjne[2]. Podstawami dla osiągnięcia bezpieczeństwa informacyjnego w opinii autorów są:

- decyzje organów władzy podjęte na podstawie istotnych i wiarygodnych informacji,
- strategiczne, niezagrożone zasoby państwa,
- niezakłócone funkcjonowanie sieci teleinformatycznych mających tworzyć krytyczną infrastrukturę teleinformatyczną państwa,
- zasada określająca, że instytucje publiczne nie naruszają prawa do prywatności obywateli,
- możliwy swobodny, dostęp obywateli do informacji publicznej,
- zagwarantowana przez państwo ochrona danych osobowych i informacji niejawnych obywateli[3].

W literaturze pojęcie, bezpieczeństwo informacyjne zdefiniowane jest, jako zbiór metod, działań i procedur podejmowanych przez uprawnione podmioty, zmierzające do zapewniania integralności gromadzonych, przechowywanych i przetwarzanych zasobów informacyjnych, ich zabezpieczenie przed nieuprawnionym ujawnieniem, modyfikacją lub zniszczeniem przez osoby trzecie mające złe zamiary w stosunku do danego podmiotu[4].

Przez bezpieczeństwo informacyjne, rozumie się także wszelkie wysiłki, służące ochronie posiadanych istotnych informacji w kontekście bezpieczeństwa. Mających wpływ na sprawne funkcjonowanie struktur społeczeństwa i państwa oraz zapewnienie

[1] S. Kowalkowski, *Niemilitarne zagrożenia bezpieczeństwa publicznego,* AON, Warszawa 2011, s. 13-15.
[2] Ministerstwo Łączności Komitet Badań Naukowych, Raport: *Cele i kierunki rozwoju społeczeństwa informacyjnego w Polsce*, Warszawa, 28 listopada 2000 r.: społeczeństwo informacyjne – [ang. Information society] – nowy system społeczeństwa kształtujący się w krajach o wysokim stopniu rozwoju technologicznego, gdzie zarządzanie informacją, jej jakość, szybkość przepływu są zasadniczymi czynnikami konkurencyjności zarówno w przemyśle, jak i w usługach, a stopień rozwoju wymaga stosowania nowych technik gromadzenia, przetwarzania, przekazywania użytkowania informacji. http://kbn.icm.edu.pl [dostęp: 25.05.2022].
[3] E. Nowak, M. Nowak, *Zarys teorii bezpieczeństwa narodowego*, Difin, Warszawa 2011, s. 103.
[4] P. Potejko, *Bezpieczeństwo informacyjne, [w:] Bezpieczeństwo państwa*, red. K. A. Wojtaszczyk, A. Materska-Sosnowska, Oficyna Wydawnicza ASPRA-JR, Warszawa 2009, s. 194.

przewagi informacyjnej poprzez zdobywanie nowych, bardziej aktualnych danych. Dezinformacyjne wobec ewentualnych przeciwników innych podmiotów lub państw[1].

W rozumieniu szerszym, bezpieczeństwo informacyjne obejmuje wszystkie procesy technologiczne począwszy od pozyskiwania, poprzez transmisję, przetwarzanie, aż do przechowywania informacji w systemach informacyjnych. Działania te stanowią kompleks przedsięwzięć zapewniających bezpieczeństwo środowiska informacyjnego[2]. Przy rozważaniu problematyki bezpieczeństwa informacyjnego, bez wątpienia należy uwzględnić, fakt, że pojęcie bezpieczeństwa informacyjnego stosuje się również do informacji spoza systemu teleinformatycznego, pojawiających się na nośnikach standardowych, np. dokumentach papierowych, mikrofilmach. Polityka bezpieczeństwa informacji w swoich ramach obejmuje proces korzystania z informacji bez względu na sposób jej przetwarzania.

Dotyka ona zarówno systemów prowadzonych tradycyjnie, czyli m.in. kartotek, dokumentów w wersji papierowej jak i systemów komputerowych[3].

Bezpieczeństwo informacyjne ze względu na liczność interakcji powinno być analizowane na kilku płaszczyznach bezpieczeństwa takich jak, państwa, organizacji, instytucji, obywatela[4].

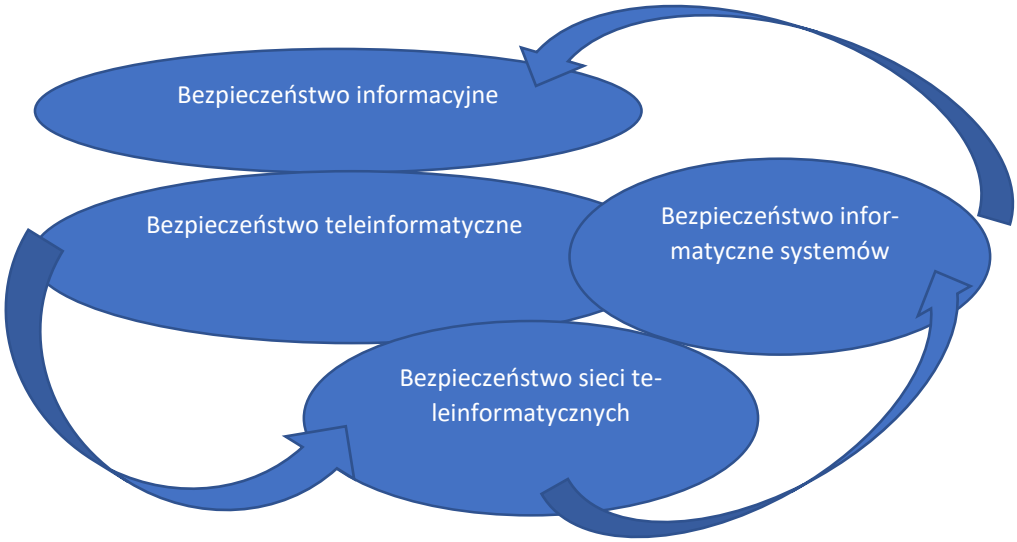
W odniesieniu do opinii ekspertów, bezpieczeństwo wyraża się we wszystkich obszarach działalności organizacji. Jego struktura jest w istocie równoważna ze strukturą funkcjonowania podmiotu, zaś bezpieczeństwo informacyjne jest umiejscawiane, obok bezpieczeństwa publicznego, ekonomicznego i militarnego w ramach szerszych pojęć bezpieczeństwa międzynarodowego i narodowego[5].Do chronionych zasobów będących w ramach bezpieczeństwa informacyjnego zalicza się:

- *sprzęt teleinformatyczny* - komputery, zasoby dyskowe, procesy, użytkowe połączenia telekomunikacyjne, teleinformatyczne, infrastruktura i urządzenia sieciowe, terminale itp.;
- *oprogramowanie* – oprogramowanie aplikacyjne, systemy operacyjne, teksty źródłowe programów, programy komunikacyjne, programy pomocnicze;

[1] M. Madej, *Rewolucja informatyczna –istota, przejawy oraz wpływ na postrzeganie bezpieczeństwa państw i systemu międzynarodowego, [w:] Bezpieczeństwo teleinformatyczne państwa*, red. M. Madej, M. Terlikowski, Polski Instytut Spraw Międzynarodowych, Warszawa 2009, s. 18-19.
[2] J. Janczak, A. Nowak, *Bezpieczeństwo…dz. cyt.*, s. 17.
[3] A. Nowak, W. Scheffs, *Zarządzanie bezpieczeństwem…dz. cyt.*, s. 40.
[4] P. Sienkiewicz, *Analiza systemowa zagrożeń dla bezpieczeństwa cyberprzestrzeni, „Automatyka*", t. 13 z 2, 2009, s. 589. http://journals.bg.agh.edu.pl/AUTOMATYKA/2009-02/Auto46.pdf [dostęp: 10.11.2022].
[5] S. Koziej, *Teoria sztuki wojennej,* „Kwartalnik BELLONA", Warszawa 2011, s. 256.

- *dane firmy* - przechowywane w plikach, w systemach bazodanowych, transmitowane, kopie zapasowe, zapisy zdarzeń, czyli logi, dane przechowywane oraz przesyłane w wersji papierowej;
- *ludzi* – administratorów i użytkowników;
- *dokumentację sprzętu*;
- *oprogramowania, lokalnych regulaminów i procedur postępowania*;
- *inne zasoby materialne* - sieci energetyczne, pomieszczenia papiery wartościowe, pomieszczenia[1]. Elementy składowe bezpieczeństwa informacyjnego prezentuje rysunek 2.3.

Rysunek 2.3. Bezpieczeństwo informacyjne w organizacji, elementy składowe



Źródło: opracowanie własne

Zakres bezpieczeństwa informacyjnego jest bardzo szeroki, odnosi się do ogółu organizacji. Uwzględnia w swej definicji materialne i niematerialne zasoby, zagrożenia o charakterze umyślnym i nieumyślnym, jakie mogą zaistnieć zarówno ze strony człowieka jak i otoczenia.

Praktyczne zastosowanie bezpieczeństwa informacyjnego obejmuje zasięgiem bezpieczeństwo samej informacji oraz bezpieczeństwo teleinformatyczne. Współzależność informacji, sieci teleinformatycznych systemów w organizacji wymaga stosownych zabezpieczeń w obszarze organizacyjnym, technicznym, proceduralnym. W aspekcie rozpatrywanego bezpieczeństwa nie mogą one pomijać słabych stron systemu, które zwięk-

[1] J. Janczak, A. Nowak, *Bezpieczeństwo informacyjne…dz. cyt.*, s. 20.

szają ryzyko zagrożenia a w następstwie osłabiają jednostkę organizacją. Szybkie reagowanie na incydenty związane z pojawiającymi się nieprawidłowościami w ochronie informacji, zwykle dokonywane przez administratorów sieci i systemów informatycznych, pozwala w sposób skuteczny udaremnić przestępstwa, a gdy już się dokonają, to ich skutki zminimalizować. Bezpieczeństwo systemu informacyjnego w dużym stopniu wymaga uporządkowania już na etapie doprecyzowania i zawężenia samej definicji.

Sposobu rozumowania i identyfikowania. W literaturze przedmiotu często dochodzi do przyrównywania informacji do danych, używania ich, jako synonimów, co w rezultacie deformuje oba pojęcia. Konkretna dana to reprezentacja fizyczna elementarnej porcji informacji. Wykorzystywana jest do rejestrowania informacji i samego jej przekazu. Informacja tymczasem jest pojęciem abstrakcyjnym oznaczającym coś, co zmniejsza entropię. Błędna interpretacja, niezauważanie różnic mają przełożenie na niejednoznaczne rozumnie pojęć systemu informacyjnego, systemu informatycznego, techniki informacyjnej, co wiąże się z nieporozumieniami (Checkland, Holwell, 2003).

Trudno doszukiwać się doskonałego systemu teleinformatycznego, który będzie absolutnym gwarantem niezawodności. Jego funkcjonalność uwarunkowana jest od działań człowieka, które na każdym etapie noszą znamiona zawodności. Począwszy od genezy systemu z uwzględnieniem fazy projektu a następnie jego wykorzystanie, aż do całkowitej jego amortyzacji (wyłączenia z użytkowania i archiwizowania).

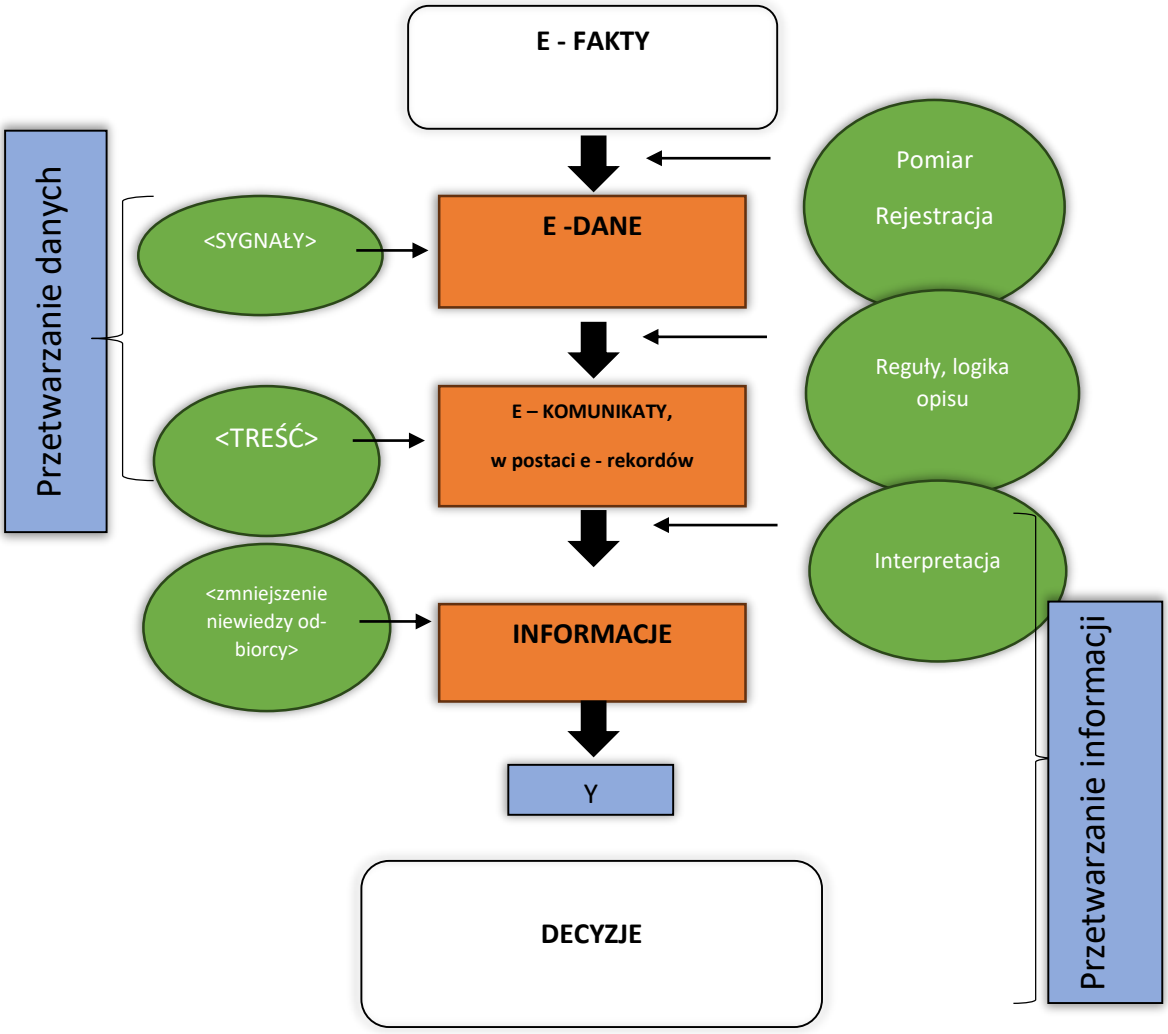
Krótko mówiąc utrzymanie na wysokim poziomie bezpieczeństwa teleinformatycznego od wszystkich użytkowników sieci i systemów wymaga bezwarunkowego przestrzegania niezbędnych procedur eksploatacyjnych zawartych w regulaminach przedstawiających warunki użytkowania wiążących się ze ścisłym zachowaniem klauzuli poufności (sytuacja dotyczy informacji o charakterze niejawnym).

Podstawowe pojęcie teorii informacji w myśl B. Langeforsa jest pojęciem złożonym, ukierunkowanym na decyzje. B. Langefors, zwraca uwagę, na fakt, że przetwarzanie danych jest ograniczone i służy do przetwarzania w obszarach ściśle wskazanych przez człowieka, natomiast przetwarzanie informacji angażuje procesy fizjologiczne mózgu, jedynie ludzie mogą je przetwarzać w swych procesach myślowych.

W ludzkim otoczeniu istnieje nieskończona liczba możliwych postaci danych, które odzwierciedlają jego stan i strukturę. Jedynie znikoma ich część jest dostępna bez-

pośrednio ludzkiemu poznaniu i tylko te stanowią sygnały informacyjne przy bezpośredniej recepcji[1]. Cykl życia systemu bezpieczeństwa informacyjnego zaprezentowany został na rysunku 2.4.

Rysunek 2.4. Cykl życia systemu bezpieczeństwa informacyjnego



Źródło: B. Langefors, (1973). Theoretical Analysis of Information Systems. 4th Edition. Lund-Philadelphia: Studentlitteratur – Auerbach Publishers

Nasuwa się, więc potrzeba zdefiniowania samego systemu, który jest każdą celowo wyodrębnioną całością, złożoną z części podsystemów, powiązań relacji między nimi jak i między każdą częścią oraz całością, którego kreatorem jest w rezultacie człowiek[2]. System to podstawowe pojęcie współczesnej nauki, a jego twórcą jest Ludwig von

[1] L. Ciborowski, *Walka informacyjna*, Wydawnictwo Adam Marszałek, Toruń 2001, s. 107.
[2] W. Flakiewicz, *Systemy informacyjne w zarządzaniu. Uwarunkowania, technologie, rodzaje*, Wydawnictwo C. H. Beck, Warszawa 2012, s. 4.

Bertalanffy. Pojęcie to wyprowadził z obserwacji podobieństw pomiędzy przyrodą, techniką i organizacją społeczeństwa ludzkiego. Na zasadzie tych podobieństw utworzył wspólne pojęcie na potrzeby opisu złożoności całości. Niezależnie od tego, czy są one tworem naturalnym czy sztucznym, ożywionym czy nieożywionym[1]. System ochrony informacji przetwarzanej w systemie informacyjnym wymaga odpowiednich organizacyjnych przedsięwzięć. Działania w systemie informacyjnym przedstawia rysunek 2.5.

Rysunek 2.5. Rodzaje działań związanych z wykonawstwem projektów systemów

Źródło: K. Liderman, Bezpieczeństwo informacyjne, PWN, Warszawa 2012, s. 65

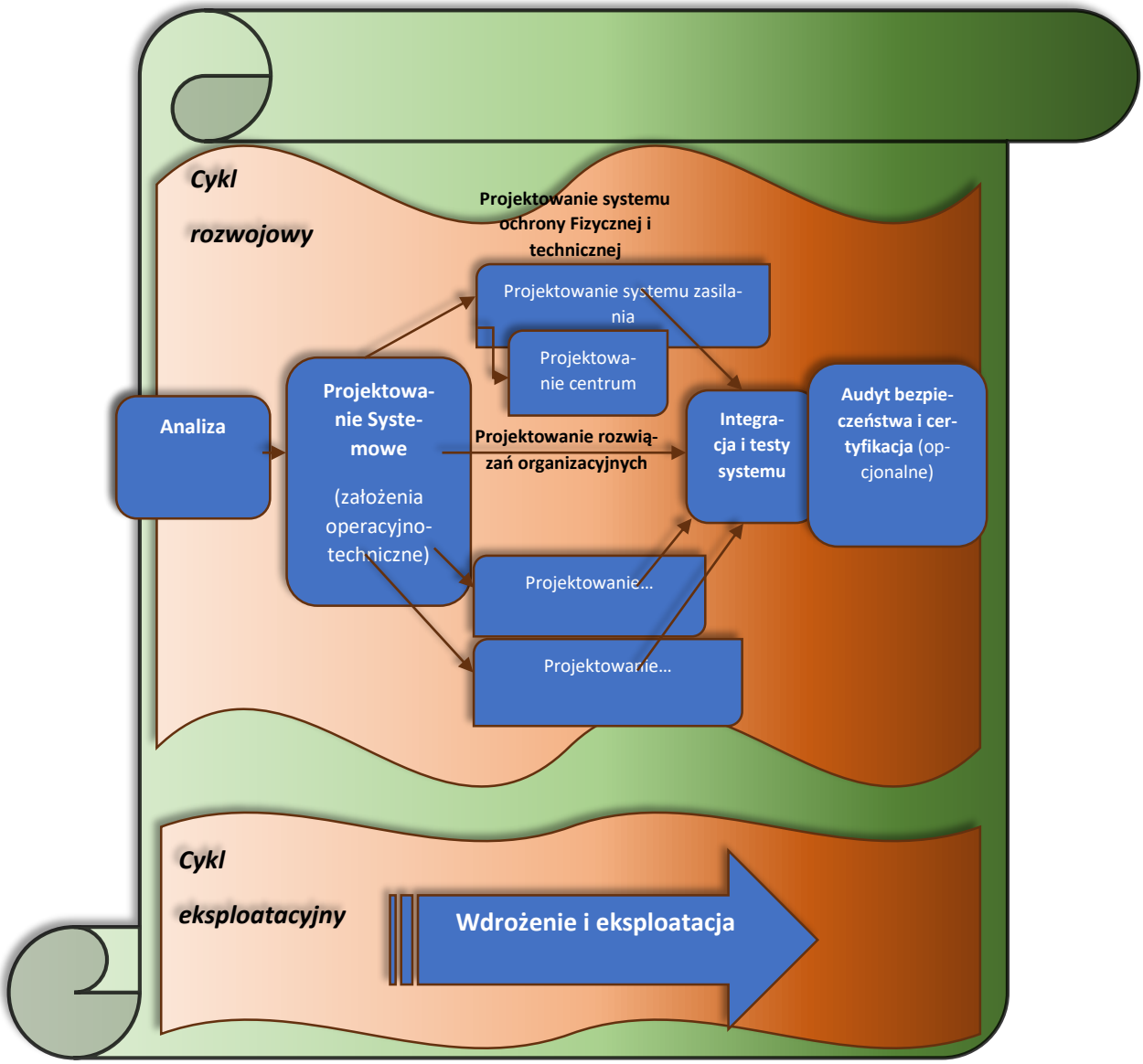
Faza rozwoju systemu wymaga wykorzystania szerokiej wiedzy eksperckiej analityków, projektantów i wdrożeniowców. Projekty i analiza powinny uwzględniać wszystkie założenia techniczne, organizacyjne podmiotu, rozpoznanie zagrożeń, oszacowanie ryzyka i planu postępowania z ryzykiem, jak również aspekty prawne. Konsolidacja podjętych działań przez zespół projektujący i budujący podlega wnikliwej ocenie oraz weryfikacji błędów, które są po ich rozpoznaniu niwelowane, a system udoskonalany, w taki sposób jak najlepiej mógł służyć jego użytkownikom a równocześnie chronić zawarte w nim informacje.

Dopiero system, który podczas audytu bezpieczeństwa umożliwia dostępność przetwarzanej informacji z zastosowaniem wszystkich należytych procedur i zachowuje

[1] M. Fertsch, *Podstawy logistyki, Instytut Logistyki i Magazynowania*, Poznań 2006, s. 20.

odpowiedni poziom tajności dla informacji niejawnych, może uzyskać certyfikację i zostać wdrożony w ramach dalszej jego eksploatacji. Cykl życia systemu bezpieczeństwa informacyjnego z uwzględnieniem poszczególnych etapów widoczny jest na rysunku 2.6.

Rysunek 2.6 Cykl życia systemu bezpieczeństwa informacyjnego

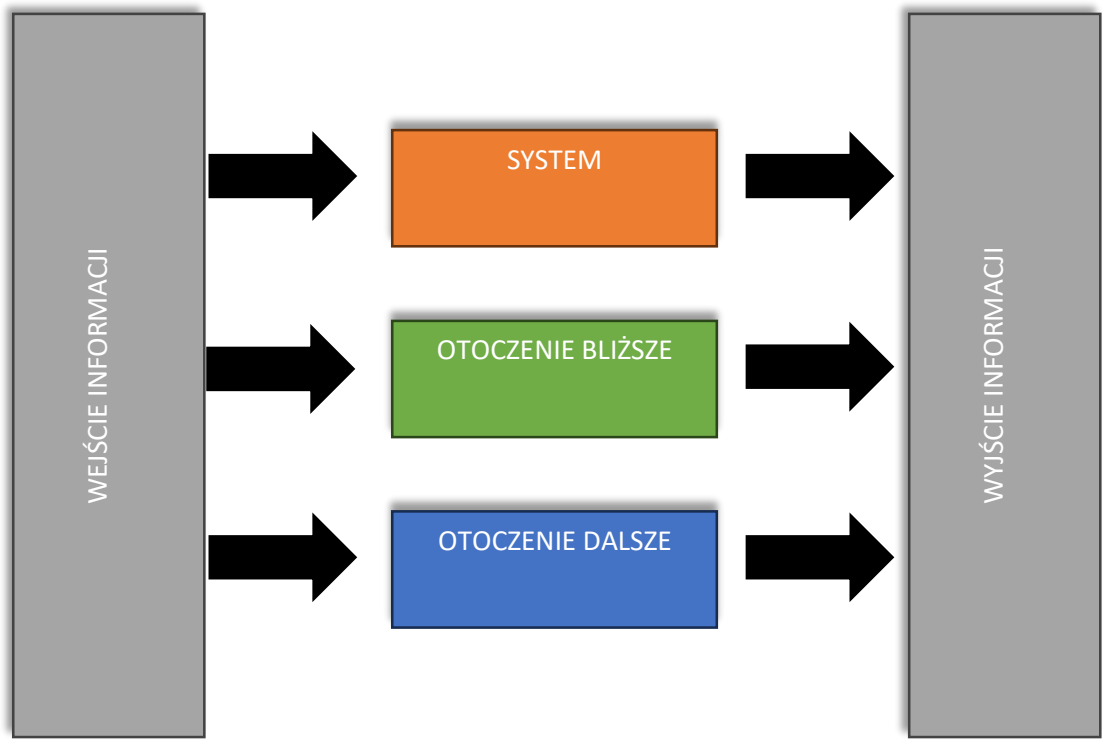


Źródło: K. Liderman, Bezpieczeństwo informacyjne, PWN, Warszawa 2012, s. 66.

W organizacji informacja charakteryzuje się dużą złożonością, w związku z powyższym należy ją rozpatrywać w kontekście związków przez jej wejście i wyjście z organizacji, uwzględniając otoczenia bliższe i dalsze, gdzie ulega transformacji. Przykład funkcjonowania systemu informacyjnego w organizacji publicznej jest zobrazowane na rysunku 2.7.

Podejście holistyczne ujmujące związek rozpatrywanego zjawiska z otaczającym światem i wewnętrzną budową Amerykanin van Bertalanffy nazwał systemem. W odpowiedzi na złożoność zachodzących procesów i zjawisk w organizacji stwierdził, iż właściwości i sposoby działania na wyższych poziomach organizacji nie dają się objaśnić przez sumowanie właściwości, sposobów działania jej części składowych, badanych oddzielnie. Poznanie zbioru części składowych i zachodzących między nimi relacji umożliwia poprzez wyższe poziomy organizacji dać się objaśnić przez jej składniki[1].

Rysunek 2.7. Otoczenie systemu informacji w organizacji



Źródło: opracowanie własne

Przedstawiany proces transformacji informacji w systemie, wskazuje, że informacja wchodząc do systemu każdej organizacji w pierwszej kolejności jest systemem informowanym a następnie podczas wychodzenia z systemu jest systemem informującym.

Do elementów kluczowych systemu należą:

- *podmioty*, a więc użytkownicy systemu mający dostęp do znajdujących się w nim informacji, prawo ich edycji itp.;

[1] W. Flakiewicz, *Systemy informacyjne w zarządzaniu…dz. cyt.*, s. 3.

- *zasoby informacyjne*, w uproszczeniu, informacje znajdujące się w systemie,
- *narzędzia* przetwarzania, przechowywania i udostępniania informacji;
- *rozwiązania systemowe* obwiązujące w danej organizacji, w ramach której system funkcjonuje (jest przez nią administrowany);
- *metainformacje,* informacje dotyczące systemu, jako całości;
- *relacje* pomiędzy poszczególnymi podmiotami[1].

Każdy z wymienionych powyżej składników ma bardzo istotny wpływ na bezpieczeństwo systemu informacyjnego w organizacji. Jest przedmiotem pożądania w walce informacyjnej. Sytuacja ta wynika z połączenia systemowego użytkowników, narzędzi, rozwiązań systemowych, metainformacji i relacji, które sprawią, że występuje między nimi zjawisko interakcji. System bezpieczeństwa informacyjnego powinien składać się z trzech ściśle ze sobą powiązanych i wchodzących w różne korelacje podsystemów. Pierwszy z nich to system bezpieczeństwa fizycznego, w którego ramach zasoby informacyjne są fizycznie oddzielone od otoczenia i stosowane są systemy kontroli dostępu, itp. np. fizyczne zabezpieczenia pomieszczeń, w których znajdują się serwery.

Dotyczy to także danych jawnych, niechronionych na podstawie regulacji ustawowych, ponieważ w takim przypadku ochrona fizyczna koncentruje się m.in. na niedopuszczaniu do zniszczenia fizycznego nośników informacji, aby zapobiec jej utraceniu. Drugim jest system bezpieczeństwa personalnego, a zatem określenia kręgu podmiotów, które posiadają różny stopień uprawnień dostępu. Możemy, zatem wyróżnić osoby, które mają fizycznie dostęp do nośników informacji np. technicy, mają dostęp do zasobów informacyjnych, czy mają uprawnienia do wprowadzania zmian w systemie np. dodawania nowych rekordów, usuwania rekordów jak i ich edytowania w formie zmiany treści.

Ostatnim z podsystemów jest system bezpieczeństwa informacyjnego w przypadku, co w obecnych czasach jest standardem, elektronicznego przetwarzania informacji, a zatem narzędzi pozwalających na zachowanie kontroli dostępu, dystrybucji uprawnień, zapobieganie nieuprawnionemu dostępowi, zapobieganie nieuprawnionej instalacji złośliwego oprogramowania itp.[2].

O nurtującym problemie utrzymania bezpieczeństwa systemu informacyjnego Winn Schwartau pisał w swojej książęce opisującej walkę informacyjną, którą zdefiniował, jako działania ukierunkowane na ochronę, wykorzystanie, uszkodzenie, zniszczenie

[1] K. Liedel, P. Piasecka, T. R. Aleksandrowicz, *Analiza…dz. cyt.,* s. 29.
[2] Tamże, s. 29-30.

informacji lub zasobów informacyjnych albo także zaprzeczenie informacjom po to, aby osiągnąć korzyści, jakiś cel lub zwycięstwo nad przeciwnikiem”.

Podobnego zdania jest L. Ciborowski, uważa on, że wszelkie działania kooperacji negatywnej wzajemnej, w których cel destrukcyjnego działania skoncentrowany jest na systemach informacyjno-sterujących przeciwnych sobie stron jest walką informacyjną, która lokuje się w grupie walk niezbrojnych pomijających fizyczne niszczenie i zagrożenie życia[1].Odnosząc się do postrzegania i poszukiwania poczucia bezpieczeństwa systemu informacyjnego warto wziąć pod uwagę model zaprezentowany przez D. Freia, który uwzględnia cztery elementy:

- *stan obsesji* w przypadku, gdy niewielkie zagrożenie postrzegane jest, jako duże;
- *stan fałszywego bezpieczeństwa,* gdy istotne zagrożenie postrzegane jest, jako niewielkie;
- *stan bezpieczeństwa*, gdy zagrożenie zewnętrzne jest niewielkie, a jego postrzeganie prawidłowe;
- *stan braku bezpieczeństwa,* gdy występuje rzeczywiste i istotne zagrożenie zewnętrzne, które postrzegane jest, jako adekwatne[2].

Indukując zwyczajowo, polityka bezpieczeństwa systemu informacyjnego powinna być kreowana poprzez władze, w przypadku uczelni wyższej rektora, w której ma być stosowana, przy wsparciu osób odpowiedzialnych za ochronę informacji znajdujących się w gestii tej jednostki. Powinna obejmować takie elementy, jak ochronę informacji niejawnych, politykę informacyjną, zasady ochrony danych osobowych, zasady ochrony tajemnicy uczelni oraz innych tajemnic zawodowych, politykę bezpieczeństwa systemu teleinformatycznego, zapobieganie przestępstwom na szkodę firmy, szczególnie fałszerstwom i oszustom, zasady ochrony fizycznej i technicznej, inne związane z bezpieczeństwem[3].

[1] L. Ciborowski, *Walka informacyjna…dz. cyt.*, s. 68.
[2] K. Liedel, *Bezpieczeństwo informacyjne w dobie terrorystycznych…dz. cyt.,* s. 8.
[3] J. Wójcik, *Kryminologiczne i kryminalistyczne problemy funkcjonowania wywiadu gospodarczego, [w:] System informacji strategicznej*, red. R. Borowiecki, M. Romanowska, Difin, Warszawa 2001, s. 352-353.

2.4. Znaczenie bezpieczeństwa systemu informacyjnego dla bezpieczeństwa narodowego

Poczucie bezpieczeństwa rozpatrywane w kontekście bezpieczeństwa narodowego, stanowi podstawę, każdego państwa autonomicznego, które w dążeniu do zapewnienia stabilnej i silnej pozycji na arenie międzynarodowej chroni swych obywateli i zasoby przed zagrożeniami. Wśród owych zasobów są miedzy innymi same informacje oraz systemy informacyjne. W opinii A. Nowaka dzisiejszy obraz cyberprzestrzeni naprowadza na konieczność traktowania tej sfery, jako jednej ze strategicznych punktów widzenia obronności kraju[1].

Uczelnia wyższa stanowi trzon rozwoju społeczeństwa i jest generatorem licznych informacji, wymagających właściwej ochrony z uwagi na dobro wszystkich użytkowników całego systemu informacyjnego, jaki w uczelni wyższej występuje. Ponadto, zapewnienie bezpieczeństwa informacyjnego w uczelni ma również przełożenie na ogólne bezpieczeństwo studentów, kadry naukowej, kadry administracyjnej i wszystkich interesariuszy z nią współpracujących.

Studium przypadku

Przykładem jak informacja może sparaliżować bezpieczeństwo i zakłócić funkcjonowanie uczelni wyższej, są e-maile, jakie 15.11.2021 r. otrzymały poznańskie uczelnie z zawiadomieniem o rzekomo podłożonym ładunku wybuchowym. Według autora wysłanej wiadomości wszystkie osoby, które nie opuszczą placówek do godz. 12:00,zginą. Poniżej treść e-maila, który napisała osoba podająca się za Łapacza Flag.
Jestem inżynierem CERT Polska i zbudowałem bombę koncentryczną. Bomba jest w waszym budynku. Detonacja w poniedziałek dokładnie w południe. Wszyscy ludzie w budynku zginą. To pewne. Uciekajcie ludzie nie ryzykujcie życia.

Powyższe informacje na swoje skrzynki e-mailowe otrzymało kilkadziesiąt instytucji w Wielkopolsce, nie tylko oświatowych. Jeżeli chodzi o pewien proces związany z ewakuacją to zawsze decyzję podejmują administratorzy. Służby mundurowe sprawdzają każdy z takich sygnałów. Przedstawiciel poznańskiej policji poinformował, że takie sygnały najczęściej mają miano fałszywych zgłoszeń. Pracownicy Uniwersytetu Ekonomicznego w Poznaniu zostali niezwłocznie ewakuowani po godzinie 10:00 z budynku

[1] A. Nowak, *Cyberprzestrzeń jako nowa jakość zagrożeń. Bezpieczeństwo Narodowe*, „Zeszyty Naukowe AON" nr 3(92), 2013, s. 5.

przy Towarowej. Uczelnia została dokładnie sprawdzona przez służby znajdujące się na miejscu zdarzenia[1]. Takie alarmy można było zaobserwować w innych polskich miastach.

Kolejnym miastem była Warszawa, w mediach społecznościowych pojawiła się informacja o alarmach bombowych na krajowych uczelniach. Zagrożoną uczelnią wyższą w tym przypadku był Uniwersytet Warszawski. Komentarz w powyższej sprawie wydała stołeczna policja oraz biuro prasowe uczelni wyższej.

Oficjalnie w dniu 1.10.2021 r. rozpoczął się nowy rok akademicki. Ten dzień nie dla wszystkich okazał się udany. W mediach społecznościowych pojawiły się informacje, że w związku z bombowymi alarmami wszystkie znajdujące się w budynku osoby zostały ewakuowane i odesłane do domów. O rzekomych bombowych alarmach pisali studenci Gdańska, Warszawy i Krakowa. O komentarz w owej sprawie została poproszona stołeczna policja oraz władze Uniwersytetu Warszawskiego. Otrzymano zwrotną odpowiedz: *My, jako policja nie potwierdzamy żadnego alarmu. Zgłoszenia, jednak są ale są one niepotwierdzone.* Taką informację udzieliła przedstawicielka biura prasowego Komendy Stołecznej Policji. Powyższej informacji nie potwierdziły władze uczelni. Budynki zostały sprawdzone a głębsze informacje nie zostały udzielone ze względów bezpieczeństwa[2].

Takie działania mają polegać na wywołaniu chaosu w uczelniach wyższych. Mimo iż, zagrożenia okazały się informacjami fałszywymi bez pokrycia jednakże w obawie o ludzkie zdrowie i życie władze uczelni, na których w związku z ich funkcją spoczywa pewna odpowiedzialność za bezpieczeństwo, życie i zdrowie osób tam przebywających, zarządzono ewakuację do czasu sprawdzenia przez policję budynków. Informacja dotycząca alarmów bombowych w rezultacie była nie prawdziwa, mino to było zagrożenie i wywołało następujące skutki:

- odwróciła skutecznie uwagę służb od innych zagrożeń, które potencjalnie mogły wystąpić;
- doprowadziła do dezorientacji pracowników i studentów znajdujących się w murach uczelnianych;
- wywołała destabilizację funkcjonowania uczelni;

[1] https://gloswielkopolski.pl/podlozone-bomby-na-poznanskich-uczelniach-rano-przyszly-emaile/ar/c1-15902903, [dostęp: 9.11.2023].
[2] https://warszawa.naszemiasto.pl/alarmy-bombowe-na-polskich-uczelniach-studenci-donosza-o/ar/c1-8478401, [dostęp: 11.11.2023].

- zmniejszyła poczucie bezpieczeństwa wśród pracowników wszystkich jednostek znajdujących się w budynku oraz studentów i nauczycieli akademickich znajdujących się w salach wykładowych będących w trakcie zajęć;
- została zwiększona ilość służb mundurowych;
- w stan gotowości zostały postawione służby medyczne;
- zostało wprowadzone zamieszanie, chaos, popłoch, niepewność, strach wśród obywateli,
- wydatkowanie środków finansowych państwa zostało zwiększone w związku z koniecznością wzięcia udziału w akcji;
- zaistniała sytuacja nadmiernie koncentrowała uwagę mediów;
- uderzyła bezpośrednio w ludzi młodych zakłócając ich kształcenie, pozyskanie wiedzy na zajęciach m.in. praktycznych mogących w późniejszych latach na pozyskanie lepiej płatnej pracy;
- doszło do dezorganizacji pracy na uczelni, ale także całego aparatu państwowego;
- państwo zostało postawione w stan gotowości.

Odwołując się do definicji, bezpieczeństwo narodowe obejmuje problematykę przeciwstawiania się wszelkim zagrożeniom wewnętrznym i zewnętrznym dla istnienia narodu i państwa. Państwo ustala zbiór wartości wewnętrznych w trosce o własne bezpieczeństwo, które jego zdaniem powinny być chronione przed wszelkimi zagrożeniami a należą do nich integralność terytorialna, biologiczne przeżycie ludzkości, narodu, jako etnicznej grupy, państwa, jako nielicznej jednostki politycznej. Wpływ ma również niezależność polityczna w zakresie ustrojowym, swobody afiliacji i samowładności. Czynniki to standard życia, rozwój społeczno-gospodarczy, system kulturalny, zakres swobód obywatelskich i praw, możliwości i perspektyw ciągłego rozwoju, stan środowiska naturalnego[1].

W społeczeństwie informacyjnym, jak wskazuje Alvin Toffler, *naczelnym czynnikiem wytwórczości i władzy człowieka* jest przepływ oraz wymiana informacji, będących fundamentem dla sprawnego funkcjonowania podmiotów, wszystkich szczebli administracji oraz życia jednostek. Sytuacja ta pokazuje istotne wyzwanie dla bezpieczeństwa narodowego, a nowy obszar potencjalnego rozpoznawania, walki interesów a nawet otwartego konfliktu zmuszającego do posiadania skutecznego systemu bezpieczeństwa to nowa technika.

[1] K. Liedel, *Bezpieczeństwo informacyjne w dobie terrorystycznych….dz. cyt.,* s. 12.

Bezpieczeństwo przyjmuje różne wymiary np. bezpieczeństwo informacyjne, polityczne, militarne, ekonomiczne, ekologiczne, społeczne, ideologiczne. Wieloaspektowość zagrożeń bezpieczeństwa wymaga od państwa całościowego działania, we wszystkich jego obszarach. Kluczowym jest jego istota i niepodzielny charakter.

Polityka bezpieczeństwa narodowego jest uwarunkowana postępem cywilizacyjnym, nowościami technicznymi i technologicznymi[1]. W Strategii Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej 2020, stanowiącej trzon dyrektyw strategicznych w odniesieniu do działalności państwa wskazano, iż bezpieczeństwo informacyjne nie jest tym samym, co bezpieczeństwo informatyczne. Często występuje łączenie znaczenia i wartości informacji wyłącznie z technologiami komputerowymi. Na podstawie art. 68, Ustawy z dnia 5 lipca 2018 r. o Krajowym Systemie Cyberbezpieczeństwa (Dz. U. poz. 1560 z póź. zm.) Rada Ministrów przyjęła Strategię Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024, jako załącznik do uchwały. W związku z powyższym, Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na wspomniane powyżej lata zastąpiła, Krajowe Ramy Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017–2022 przyjęte uchwałą nr 52/2017 Rady Ministrów z dnia 27 kwietnia 2017 r. w sprawie Krajowych Ram Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017–2022. Zamierzeniem dokumentu jest określenie strategicznych celów oraz wdrożenie środków regulacyjnych i politycznych. Ostateczną wizją przedsięwzięcia jest uzyskanie wysokiego poziomu cyberbezpieczeństwa[2].

W szczególności realizacja celów strategicznych powinna wpływać na podniesienie bezpieczeństwa narodowego polegającego na zwiększeniu skuteczności działań wymiaru sprawiedliwości oraz organów ścigania w wykrywaniu jak i zwalczaniu cyberprzestępstw, działań mających charakter hybrydowy, terrorystyczny, szpiegowski w cyberprzestrzeni. Owa Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024 jest spójna. Prowadzone są działania dotyczące systemów teleinformatycznych operatorów infrastruktury krytycznej. Uwzględnia również potrzeby zapewnienia zdolności

[1] K. Liedel, *Bezpieczeństwo informacyjne…dz. cyt.*, s. 17.
[2] Dotyczy operatorów usług kluczowych, o których mowa w art. *5 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa z późn zm*.

Siłom Zbrojnym Rzeczypospolitej Polskiej w układzie krajowym, koalicyjnym, sojuszniczym do prowadzenia militarnych działań w przypadku zagrożenia cyberbezpieczeństwa mającego spowodować konieczność działań obronnych[1].

W odniesieniu do realistycznej teorii bezpieczeństwa narodowego utrzymanie tegoż bezpieczeństwa w aspekcie informacyjnym powinno się opierać na przesłankach tj:

- zwiększeniu ochrony systemów informacyjnych będących we własnym posiadaniu,
- przygotowanie różnych opcji form obrony przed atakami, przy wykorzystaniu informacyjnych, konwencjonalnych wojskowych środków rażenia,
- stałe kontrolowanie i ocena słabości systemów informacyjnych potencjalnych przeciwników oraz działania uwzględniające możliwość wtargnięcia do ich systemów,
- rozwój metod szacowania poniesionych strat w tym strat informacyjnych.

Zastosowanie teorii liberalnej bezpieczeństwa narodowego, ochrona systemów informacyjnych polegać będzie na takich czynnikach jak, tworzenie globalnych instytucji, porozumień zapobiegających wojnie informacyjnej i zwiększeniu poziomu współzależności oraz powiązań systemów informacyjnych państw, których celem będzie przeciwdziałanie zagrożeniom[2].

Wprowadzenie równowagi pomiędzy teorią realistyczną bezpieczeństwa narodowego a teorią liberalną wymaga m.in. powołania porozumień przeciwko działaniom wojennym, zwiększenia poziomu ochrony systemów informacyjnych oraz posiadanie świadomości, że jakieś własne słabe strony istnieją[3]. Dla bezpieczeństwa państwa niezbędne jest wprowadzenie polityki bezpieczeństwa informacji. Fakt ten ma zapewnić ochronę istniejących systemów takie stwierdzenie przytoczył K. Liedel. Środki bezpieczeństwa mające miano pozytywnych powinny uwzględniać m.in:

- większość dochodu państwa zostanie uzyskana z szeroko rozumianego sektora informacyjnego;
- procesy decyzyjne w innych sektorach gospodarki i życia społecznego uzależnione będą od systemów przetwarzania i przesyłania informacji;

[1] *Monitor Polski Dziennik Urzędowy Rzeczypospolitej Polskiej*, Warszawa dnia 30 października 2019 r. Poz. 1037 Uchwała Nr 125 Rady Ministrów z dnia 22 października 2019 r. *w sprawie Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024*, s. 6.
[2] *Zagrożenia dla bezpieczeństwa informacyjnego państwa (identyfikacja, analiza zagrożeń i ryzyka*), „Raport z badań AON", t. 2, 2004, s. 109.
[3] K. Liedel, *Bezpieczeństwo informacyjne w dobie terrorystycznych….dz. cyt.*, s. 21.

- informacja i wynikająca z niej wiedza oraz technologie informatyczne są podstawowym czynnikiem wytwórczym[1].

Z punktu widzenia bezpieczeństwa narodowego zasoby informacyjne stanowią elementy bardzo wrażliwe. Ich naruszenie zakłóca funkcjonowanie państwa oraz tworzy zagrożenia dla bezpieczeństwa[2].

Podsumowując widać, że znaczenie bezpieczeństwa państwa jest podstawą utrzymania pokoju a co za tym idzie stabilizacji w państwie. Hakerzy coraz lepiej sobie radzą w rozpracowywaniu systemów informacyjnych a tym samym wywieraniu realnego wpływu na politykę, obronę militarną, ochronę środowiska, gospodarkę oraz inne sfery życia społecznego w państwie. Stosowanie odpowiednich zabezpieczeń systemowych, procedur a przede wszystkim natychmiastowe reagowanie na incydenty znacznie podwyższa stopień bezpieczeństwa informacyjnego.

2.5. Źródła prawa dotyczące bezpieczeństwa informacyjnego

Konstytucja Rzeczypospolitej Polskiej uchwalona w dniu 2 kwietnia 1997 r. przez Zgromadzenie Narodowe implikuje ład w kraju. W swojej treści bezpośrednio nie odnosi się w bezpośredni sposób do bezpieczeństwa informacyjnego jednakże art. 31. stanowi, że wolność człowieka podlega ochronie prawnej. Obowiązek Konstytucyjny człowieka do poszanowania prawa oraz wolności jak i fakt, że nikt nie może być zmuszony do czynienia tego, czego prawo mu nie nakazuje ma swoje odzwierciedlenie w bezpieczeństwie systemu informacyjnego w uczelni wyższej. Podmiotem w organizacji publicznej jest czynnik ludzki, który wymaga ochrony prawnej przed mogącymi wystąpić zagrożeniami.

W powyżej omawianym akcie normatywnym znajdują się także regulacje, mówiące bezpośrednio o ograniczeniach w zakresie korzystania z konstytucyjnych praw i wolności. Mogą być one ustanawiane tylko w ustawie, gdy są konieczne w demokratycznym państwie. Mają posłużyć dla jego bezpieczeństwa, porządku publicznego, ochrony środowiska, zdrowia i moralności publicznej, praw i wolności innych osób.

Prawidłowe funkcjonowanie uczelni wyższej wymusza konieczność gromadzenia jawnych i niejawnych informacji o jej wszystkich użytkownikach. Władze uczelni sprawują pieczę nad pełnym bezpieczeństwem uczelni, jako organizacji zatrudniającej pra-

[1] K. Liedel, *Bezpieczeństwo informacyjne w dobie…dz. cyt.*, s. 31.
[2] K. Liedel, P. Piasecka, T. R. Aleksandrowicz, *Analiza…dz. cyt.,* s. 28.

cowników oraz kształcącej studentów również bezpieczeństwa mającego charakter informacyjny. Już na etapie przyjmowania dokumentów aplikujących do pracy na uczelni oraz kandydatów na kierunki organizowane przez podmiot powinny być one objęte szczególną ochroną i szczególnymi procedurami rekrutacyjnymi czy w przypadku pozyskiwania pracowników naukowy lub administracyjnych procedury konkursowej.

Ochrona ta wedle Konstytucji RP podnosi także fakt, że nikt nie może być obowiązany inaczej niż na podstawie ustawy do ujawniania informacji dotyczących jego osoby. Analizując art. 51 Konstytucji RP władze publiczne, w tym przypadku rektor, prorektorzy czy kierownicy jednostek organizacyjnych nie mogą pozyskiwać, gromadzić i udostępniać innych informacji o obywatelach niż niezbędne w demokratycznym państwie prawnym. Artykuł ten również mówi, że każdy ma prawo dostępu do dotyczących go dokumentów urzędowych oraz zbiorów danych. Konstytucja RP dopuszcza ograniczenie tego prawa, jednakże musi to ograniczenie określać ustawa. W sytuacji, gdy obywatel ma poczucie, że pozyskane informacje dotyczące jego osoby noszą znamiona nieprawdziwych, zebranych w sposób nieprawidłowy z ustawą ma prawo do żądania sprostowania lub usunięcia nieprawdziwych informacji.

Należy zaznaczyć, że według art. 87 Konstytucji Rzeczypospolitej Polskiej wszelkimi źródłami powszechnie obowiązującego prawa RP są takie dokumenty jak, Konstytucja, Ustawy, Ratyfikowane umowy międzynarodowe, Rozporządzenia.

Źródłami powszechnie obowiązującego prawa w RP są na obszarze działania organów, które je ustanowiły, akty prawa miejscowego[1]. Zgodnie z ustawą z dnia 20 lipca o ogłoszeniu aktów normatywnych i innych aktów prawnych jest konieczność ich ogłoszenia, aby weszły w życie[2]. J. Janczaka i A. Nowaka uważa, że prawo ma za zadanie ukazanie ważnej roli przepisów i zaakcentowanie istnienia nowych rozwiązań prawnych skierowanych w stronę ludzkiej jednostki mającej dostęp do Internetu i komputera jak również jednostek organizacji publicznej i niepublicznej będącej uczelnią wyższą. Autorzy dowodzą, że w skład polskiego porządku prawnego dotyczącego bezpieczeństwa informacyjnego źródeł prawa wymienionych w art. 84 Konstytucji RP wchodzi cały dorobek prawny Unii Europejskiej[3]. Przeświadczeniem tego jest fakt przynależności Polski

[1] *Konstytucja Rzeczypospolitej Polskiej* uchwalona w dniu 2 kwietnia 1997 r. przez Zgromadzenie Narodowe, przyjęta przez naród w referendum konstytucyjnym w dniu 25 maja 1997 r., podpisana przez Prezydenta Rzeczypospolitej Polskiej 16 lipca 1997 r., tekst ogłoszony w Dz. U. 1997, nr 78, poz. 483.
[2] Ustawa z dnia 20 lipca 2000 r. *o ogłaszaniu aktów normatywnych i niektórych innych aktów prawnych* (Dz. U. 2019, poz. 1461.).
[3] J. Janczak, A. Nowak, *Bezpieczeństwo informacyjne…*dz. cyt., s. 24-26.

do Unii Europejskiej. Sytuacja ta spowodowała, że państwo w państwie członkowskim Wspólnoty Europejskiej obowiązuje prawo wspólnotowe, zgodne z prawem i normami wspólnotowymi.

Prawne regulacje mające ścisły związek z bezpieczeństwem systemów informacyjnych w pewien sposób można poszerzyć o inne standardy, mające ograniczać ryzyko w organizacji publicznej. Zwiększeniu efektywności polityki bezpieczeństwa informacyjnego ma służyć prawna ochrona informacji zawarta w dokumentach normatywnych. Wdrażanie Systemu Bezpieczeństwa Informacji powinno być zgodne z literą prawa[1]. Wszelkie treści mające w zamyśle podkreślić wagę problematyki dotyczącej bezpieczeństwa informacyjnego można odnaleźć m.in. w Strategii Bezpieczeństwa Narodowego RP[2], jak również w rządowym dokumencie tj. Rządowy program ochrony cyberprzestrzeni Rzeczpospolitej Polskiej na lata 2009/2011[3]. Tematyka bezpieczeństwa informacyjnego regulowana jest polski system prawny, Konstytucję RP oraz Biała Księga Bezpieczeństwa Narodowego RP. Ochrona informacji niejawnych jest szczególną dziedzina bezpieczeństwa informacyjnego. Treści informacji tego typu, których nieuprawnione ujawnienie może być niekorzystne i spowodować szkodliwe skutki dla Rzeczpospolitej Polskiej[4].

W rozpatrywaniu terminu dotyczącego bezpieczeństwa informacyjnego konieczne jest odniesienie do norm PN-ISO/IEC 27001:2017-06 oraz PN-ISO/IEC 17799:2007[5]. Termin ten jest tam opisany, jako zachowanie dostępności, poufności, in-

[1] K. Liderman, *Bezpieczeństwo informacyjne…dz. cyt.*, s. 23.
[2] *Strategia Bezpieczeństwa Narodowego RP* w pkt 3.8. stanowi: Zwalczanie zagrożeń rządowych systemów teleinformatycznych i sieci telekomunikacyjnych ma na celu przeciwdziałanie przestępczości komputerowej oraz innym wrogim działaniom wymierzonym w infrastrukturę telekomunikacyjna, w tym zapobieganie atakom na elementy tej infrastruktury. Szczególne znaczenie ma ochrona informacji niejawnych przechowywanych lub przekazywanych w postaci elektronicznej, http://www.iniejawna.pl/pomoce/przyc_ pom/SBN_RP.pdf, [dostęp: 17.12.2022].
[3] K. Liderman, *Bezpieczeństwo informacyjne…dz. cyt.*, s. 24.
[4] *Biała Księga Bezpieczeństwa Narodowego RP*, http://www.spbn.gov.pl/, [dostęp: 19.12.12.2022].
[5] PN-ISO/IEC 27001:2017-06 *Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji* – Zakres: przedstawiono wymagania dotyczące ustanowienia, wdrożenia, eksploatacji, monitorowania, przeglądu, utrzymania i doskonalenia udokumentowanego systemu zarządzania bezpieczeństwem informacji (SZBI) w całościowym kontekście ryzyk biznesowych i określono wymagania dotyczące wdrożenia zabezpieczeń dostosowanych do potrzeb pojedynczych organizacji lub ich części, http://www.pkn.pl/, [dostęp:19.12.2022].

tegralności, jednakże należy uwzględnić własności związane z niezawodnością, niezaprzeczalnością, autentycznością. ISO/IEC 17799[1], jest to norma mająca swoje odniesienie do bezpieczeństwa informacji, dostarczając takich rozwiązań, które dają prosty ogląd na zagadnienia mające związek przy tworzeniu procedur bezpieczeństwa[2].

Bezpieczeństwo informacji podlega licznym regulacjom prawnym. A. Nowak i W. Scheffs pokazują, że bardzo ważne są takie ustawy jak:

- ustawa o ochronie danych osobowych,
- ustawa o ochronie informacji niejawnych,
- ustawa o prawach autorskich i prawach pokrewnych,
- ustawa o dostępie do informacji publicznej[3].

Dla każdego zakresu działania organizacji istnieje w Polsce ponad dwieście aktów prawnych mających swoje odniesienie do ochrony informacji[4].

2.6. Diagnoza systemu informacyjnego w uczelni wyższej

Uczelnia wyższa jest autonomiczna na zasadach określonych w ustawie, posiada ona osobowość prawną. Uczelnia prowadzi działalność w swojej siedzibie może również prowadzić działalność w ośrodkach pozamiejscowych (poza siedzibą w swojej filii). Podstawowymi zadaniami, nad jakimi powinna skupić się działalność realizowana przez uczelnię to:

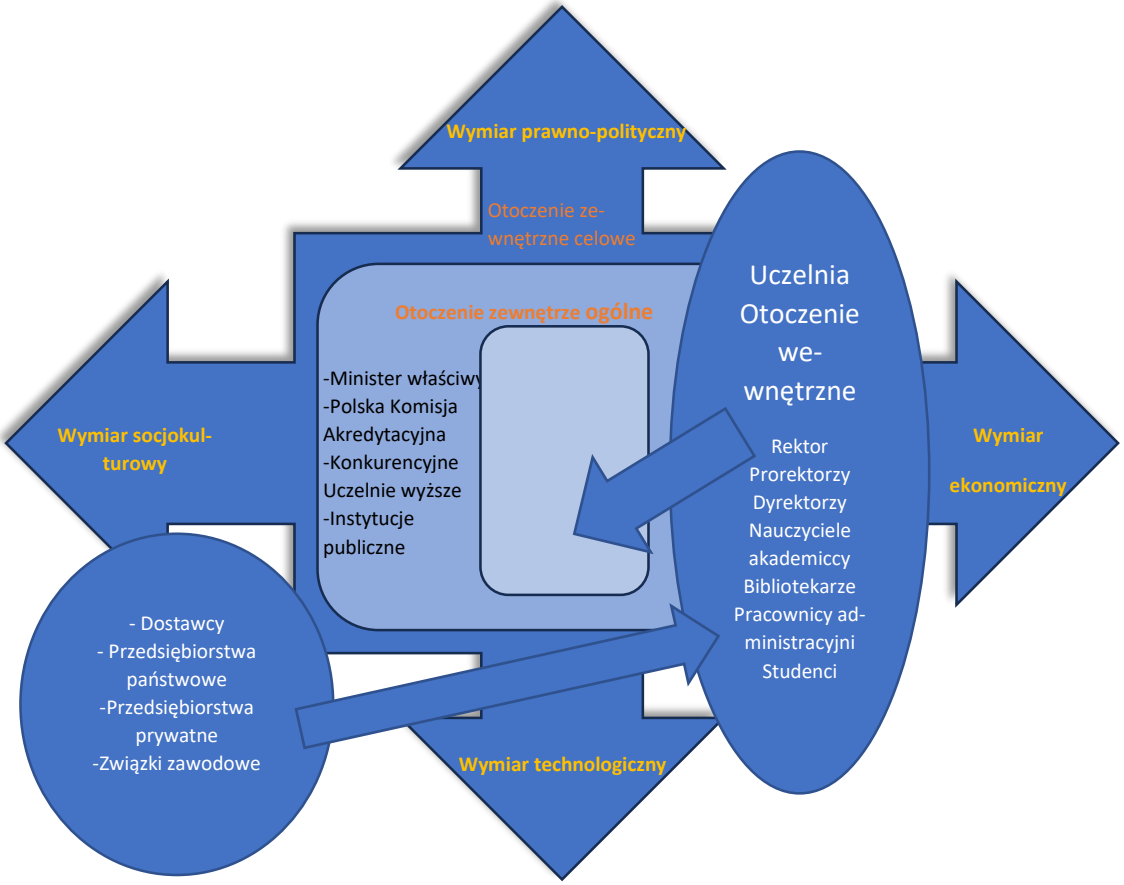
- prowadzenie kształcenia na kierunkach realizowanych wewnątrz uczelni (studia stopnia pierwszego, drugiego, jednolite magisterskie, podyplomowe, doktoranckie);
- prowadzi działalność naukową, świadczy usługi badawcze, jak i transfer wiedzy i technologii do gospodarki;
- kształcenie jak również promowanie kadr uczelni;

[1] PN-ISO/IEC 17799:2007 *Technika informatyczna – Techniki bezpieczeństwa – Praktyczne zasady zarządzania bezpieczeństwem informacji* – Zakres: Przedstawiono zalecenia i ogólne zasady dotyczące inicjowania działań, wdrażania, utrzymania i doskonalenia zarządzania bezpieczeństwem informacji w organizacji. Cele stosowania zabezpieczeń przedstawione w normie są powszechnie akceptowanymi praktykami zarządzania bezpieczeństwem informacji, http://www.pkn.pl/, [dostęp:19.12.2022].
[2] A. Nowak, W. Scheffs, *Zarządzanie bezpieczeństwem…dz. cyt.*, s. 35.
[3] A. Nowak, W. Scheffs, *Zarządzanie…dz. cyt.*, s. 6.
[4] Jako przykład może posłużyć obowiązująca podmioty prowadzące księgi rachunkowe Ustawa o Rachunkowości, której cały rozdział ósmy dotyczy zagadnienia ochrony danych, w tym szczegółowo reguluje tematykę przechowywania danych, ich przetwarzania i udostępniania. *Zob. Ustawa z 29.09.1994 r. o rachunkowości* (Dz. U. z 2009 r. nr.152, poz.1223 z póz. zm.).

- w przypadku osób niepełnosprawnych prowadzi działania, aby umożliwić pełny udział w procesie przyjęcia na uczelnię (za pośrednictwem rekrutacji w przypadku studentów i konkursów w przypadku osób chcących być uczestnikami konkursów w ramach, których osoby posiadające najlepsze kwalifikacje będą mogły przyjść do kolejnego etapu a w rezultacie otrzymają pracę), prowadzeniu działalności naukowej;
- wkład w wychowanie studentów w poczuciu odpowiedzialności za państwo polskie, narodową tradycję, poszanowanie praw człowieka i umacnianie zasad demokracji;
- upowszechnienie i pomnażanie osiągnięć nauki i kultury, poprzez procesy tj. gromadzenie i udostępnianie zbiorów bibliotecznych, informacyjnych oraz archiwalnych;
- ważną kwestia w przypadku studentów jest stworzenie dla nich odpowiednich warunków do rozwoju zdrowego stylu życia poprzez wytyczne realizowania w ramach swojego planu studiów z uczestnictwa w kulturze fizycznej[1].Poniżej został przedstawiony zarys organizacji uczelni wyższej, uzupełniony informacjami pochodzącymi ze środowiska wewnętrznego i zewnętrznego uczelni wyższej, odwołuje do niego rysunek 2.8.

[1] Ustawa z dnia 20.07.2018 r., *Prawo o szkolnictwie wyższym i nauce* (Dz.U. z 2018 r., poz. 1668)., https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20180001668/U/D20181668Lj.pdf [dostęp: 15.02.2022].

Rysunek 2.8. Otoczenie uczelni wyższej



Źródło: opracowanie własne

Zasadniczą rolę w uczelni wyższej tworzą studenci oraz pracownicy. Nad uczelnią wyższą m.in. sprawuje nadzór Polska Komisja Akredytacyjna mająca na celu zapewnienie, jakości uzyskania efektów kształcenia w szkolnictwie wyższym[1].

Należy zaobserwować złożoność środowiska uczelnianego, są widoczne różne podmioty pełniące nadzór z jednej strony pedagogiczny, zaś inne są organami prowadzącymi szkołę wyższą, jeszcze inne maja cel, aby wspierać proces edukacji studentów, aby był jak na najwyższym poziomie, wzbogacają ofertę kierunków proponowanych, są miejscem praktyk studenckich, chronią interesy pracowników, wspierają rozwój nauczycieli akademickich oraz pracowników niebędących nauczycielami akademickimi (kadra administracyjna), stoją na straży zdrowia i bezpieczeństwa wspomnianych grup pracowników i studentów.

Otoczenie organizacyjne uczelni wyższej niezmienne dostosowanie jest do wewnętrznych i zewnętrznych uwarunkowań jednostki. Owe uwarunkowania są kreowane

[1] https://www.pka.edu.pl/2019/04/14/polska-komisja-akredytacyjna/, [dostęp: 19.11.2023].

przez ewaluujące wymagania prawno-polityczne, postępy techniczne, aspekty mające zakres ekonomiczny. Ważną kwestia jest ciągły postęp techniczny, rozwój cyfryzacji, demografia, wartości społeczne, są to cechy w obrębie, których funkcjonuje uczelnia wyższa. Uczelnie wyższe w związku z lepszym i szybszy przepływem informacji wprowadziły dla studentów i pracowników wirtualną uczelnię oraz trwają wdrożenia zmiany systemu na USOS mając nadzieję, że ten system sprosta oczekiwaniom zarówno pracowników jak i studentów. System ten zawiera dane dotyczące studentów oraz cały przebieg studiów m.in. zaliczenia, stypendia, urlopy dziekańskie itd.

System ten to nic innego jak indeks studenta. Bardzo trudnym tematem w takich organizacjach publicznych jak uczelnia wyższa są środki finansowe pochodzące z budżetu państwa jest to tzw. subwencja dydaktyczna, która przypisana jest do studenta, ale tylko studiów stacjonarnych. W przypadku studentów studiów niestacjonarnych takiej dopłaty z Ministerstwa nie ma i student studiujący na kierunkach niestacjonarnych musi we własnym zakresie ponieść koszty swojego kształcenia. Na uczelni wyższej jednostki są samofinansujące w związku z powyższym czasami jest ogromny problem z zapewnieniem wszystkich potrzeb niezbędnych do efektywniejszego kształcenia studentów. Brak jest właściwych narzędzi teleinformatycznych, zapewnienie odpowiedniej infrastruktury, czyli w pełni wyposażonych sal komputerowych i odpowiednie zabezpieczenie systemów. Często do dydaktyki i kształcenia studentów używany jest przestarzały sprzęt mający starsze oprogramowania.

Wszystkie te wyżej wymienione czynniki mają ogromny a przede wszystkim bezpośredni wpływ na zachowanie bezpieczeństwa. Partycypacja społeczeństwa w zarządzaniu uczelnią wyższą oczekuje od kierownika jednostki sprzężenia zwrotnego zachodzącego w interpersonalnej komunikacji, jako transakcji stanowiącej proces oddziaływania wzajemnego. Komunikujący, pełni tutaj dwa zadania jedno polega na wysyłaniu przekazu, zaś drugie na jednoczesnym śledzeniu reakcji na swoją komunikację[1]. Zarządzanie uczelnią wyższą powinno polegać przede wszystkim na koalicyjności i przestrzeganiu zasad dotyczących spraw etycznych. Pomijając te wartości dobra organizacja w tym przypadku nie będzie skuteczna i poprowadzi do chaosu.

[1] M. Majchrzak, *Czy jest możliwe szkolne porozumiewanie się bez barier?, [w:] Czy polska szkoła ceni dobrą rozmowę? Komunikacja interpersonalna w edukacji,* red. W. Heller, Poznań-Kalisz 2011, s.101.

Właściwa organizacja jednostki, wprowadza wysoki poziom bezpieczeństwa studentów, pracowników a wysoki poziom kształcenia ma przełożenie na zarządzanie bezpieczeństwem informacyjnym [1].Bezpieczeństwo systemu informacyjnego powinno być celem nadrzędnym w działaniach zarządczych odnoszących się do kierowania każdą organizacją. Szczególnie ważnym narzędziem w zarzadzaniu uczelnią wyższą jest system informacyjny za pomocą, którego władze uczelni wyższej oraz pracownicy i studenci są w stanie w szybki i łatwy sposób dokonywać procesów weryfikacji sprawności i poprawności funkcjonowania wyżej wskazanej jednostki będącej przedmiotem rozważań. Pełny dostęp do znajdujących się w systemie informacji wymaga udzielenia uprawnień poprzez weryfikację pracownika, jego zakresu powierzonych mu obowiązków wynikających ze specyfiki pracy na zajmowanym stanowisku.

Patrząc z perspektywy liczby użytkowników i mnogości dostępnych zasobów fakt ten w dużym stopniu sprzyja systematycznym i przypadkowym błędom wynikającym ze sposobu użytkowania i przeszkolenia nowych pracowników podejmujących działania systemu informacyjnego. Władze uczelniane powinny *stać na straży* propagowania, motywowania, wdrażania dobrych praktyk u pracowników mających na celu nabycie wiedzy, wykorzystanie jej w odpowiedni sposób oraz przekazywanie i dzielenie się nią z innymi osobami z reguły będącymi na samym początku swojej ścieżki zawodowej[2]. Poniżej zostały wymienione działania związane z problematyką bezpieczeństwa informacyjnego. Działania te wymagają szczególnych form postępowania czyli pozyskiwanie, gromadzenie, przechowywanie, aktualizację, przetwarzanie, przesyłanie, archiwizację.

W uczelni wyższej bezpieczeństwo systemu informacyjnego powinno charakteryzować się interdyscyplinarnością a w szczególności obejmować takie środowiska jak, informatyczne, techniczne, zarządcze, ekonomiczne, finansowe, organizacyjne z uwzględnieniem zasobów ludzkich w postaci pracowników, studentów a na koniec otoczenie społeczne i prawne.

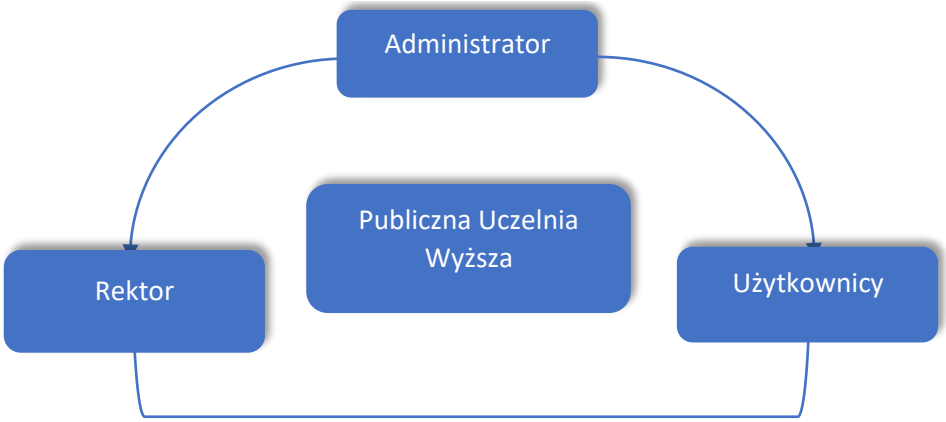
Istnieje prawdopodobieństwo, że nie wszystkie jednostki w pełni są na to przygotowane, ponieważ mają charakter fragmentaryczny, wybiórczy i dotyczący tylko i wyłącznie niektórych obszarów związanych bezpośrednio z zarządzaniem informacją. Od-

[1] M. Majchrzak, *Effective Public Management in Local Government, „European Journal of Science and Research",* 1/2017, s. 50.
[2] J. Wołejszo, *Formy szkolenia obronnego w podsystemie niemilitarnym,* „ Studia Kaliskie" t. 6, 2018, s. 51.

wołując się do literatury tematyki ściśle związanej z bezpieczeństwem systemu informacyjnego i poglądów autorów na temat zagadnień są one w dużej mierze zbieżne i uznane za nieodłączny element funkcjonowania uczelni wyższej, jako szeroko postrzeganej organizacji. W poglądach pojawiają się tylko różnice dotyczące proponowanych rozwiązań, wdrożenia oraz wszelkich działań prowadzących do wykorzystania systemów.

Uczelnia wyższa, jako organizacja publiczna w swojej strukturze zaprezentowany system współtworzą użytkownicy, czyli takie grupy jak nauczyciele akademiccy, kadra administracyjna, studenci. Na czele systemu informacyjnego stoją bezpośrednio władze uczelni wyższej wraz z administratorem. Strukturę użytkowników systemu informacyjnego w uczelni wyższej prezentuje rysunek 2.9.

Rysunek 2.9. System informacyjny funkcjonujący w uczelni wyższej



Źródło: opracowanie własne

Powyższy model systemu informacyjnego działający w uczelni wyższej pokazuje hierarchiczny schemat organizacyjny i powoduje zróżnicowanie jego użytkowników. Mając na celu weryfikację przyjętych hipotez, została dokonana analiza zebranego materiału empirycznego dotyczącego organizacji oraz zasad mających wpływ na użytkowanie systemu informacyjnego w uczelni wyższej.

Pytania zostały w taki sposób skonstruowane, aby respondenci mieli możliwość na udzielenie jednej z pięciu odpowiedzi. Skala odpowiedzi miała przedział od 1-5. Na pytanie 1 wyjaśniając, że skala 1 - oznacza *najrzadziej*, zaś 5 – *oznacza najczęściej*.

1. *W jaki sposób najczęściej Państwo przekazujecie i odbieracie informacje w uczelni wyższej?*

a) Kanał obiegu informacji – system wewnętrzny uczelni wyższej (Wirtualna Uczelnia, Dziekanat10/USOS)

W całym badaniu wzięło udział 1500 respondentów, po 500 osób z każdej grupy (nauczyciele akademiccy, kadra administracyjna, studenci (różne kierunki).

W tabeli 2.1 zaprezentowano rozkład odpowiedzi na temat wykorzystanego w uczelni wyższej kanału obiegu informacji, jakim jest uczelniany system wewnętrzny (wirtualna uczelnia, dziekanat10/USOS). Zostały porównane 2 grupy respondentów nauczyciele akademiccy i kadra administracyjna.

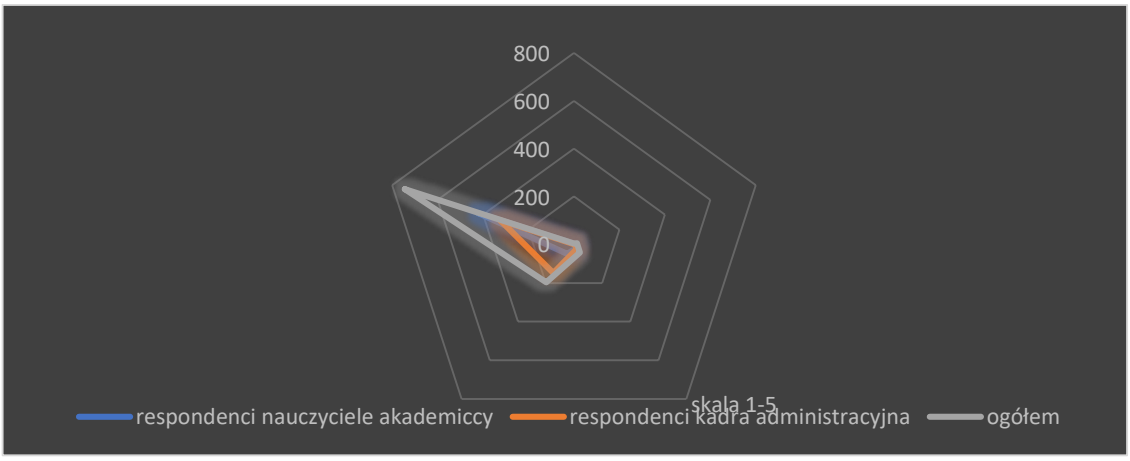
Tabela.2.1. Odpowiedzi respondentów (nauczycieli akademickich i kadry administracyjnej) na temat najczęściej wykorzystanego kanału służącego do przekazywania informacji, jakim jest (wirtualna uczelnia, dziekanat10/USOS)

Odpowiedzi badanych osób • **Zastosowany rodzaj kanału obiegu informacji (wirtualna uczelnia, dziekanat10/USOS)**									
Osoby poddane badaniu	**Respondenci nauczyciele akademiccy**			**Respondenci kadra administracyjna**			**OGÓŁEM**		
Ocena od 1-5	***liczba wskazań***	***udział procentowy***	***ocena średnia***	***liczba wskazań***	***udział procentowy***	***ocena średnia***	***liczba wskazań***	***udział procentowy***	***ocena średnia***
1	3	0,6%	0,006	0	0	0,0	3	0,3%	0,003
2	8	1,6%	0,03	5	1%	0,02	13	1,3%	0,2
3	20	4%	0,12	22	4,4%	0,13	42	4,2%	0,13
4	49	9,8%	0,39	148	29,6%	1,18	197	19,7%	0,79
5	420	84%	4,2	325	65%	3,25	745	74,5%	3,72
	500	**100%**	**4,75**	**500**	**100%**	**4,58**	**1000**	**100%**	**4,84**

Źródło: Opracowanie własne na podstawie własnych badań

W badaniu wzięło udział 500 osób zatrudnionych na stanowisku, nauczycieli akademickich oraz 500 osób zatrudnionych na stanowisku kadry administracyjnej. Wszystkie wyżej wskazane osoby poprawnie udzieliły odpowiedzi w ilości 100%. Nie doszło do sytuacji, w której odpowiedzi zostały błędnie wskazane. W przypadku nauczycieli akademickich najwyższą (najczęstszą) odpowiedź odnośnie kanału przekazywania informacji, jaką jest *wirtualna uczelnia, dziekanat10/USOS,* udzieliło 420 respondentów to jest 84%. Najniższą odpowiedź (najrzadziej) korzysta z tej drogi przekazu informacji 3 osoby to jest 0,6%. Kadra administracyjna zadeklarowała najwyższą (najczęstszą) drogę przesyłu informacji w ilości 325 respondentów to jest 65%. Liczba wskazań dla kadry administracyjnej wynosiła 0.

Wykres 2.1. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy kadra administracyjna na temat najczęściej wykorzystywanego kanału służącego do przekazywania informacji, jakim jest (wirtualna uczelnia i dziekanat10/USOS)



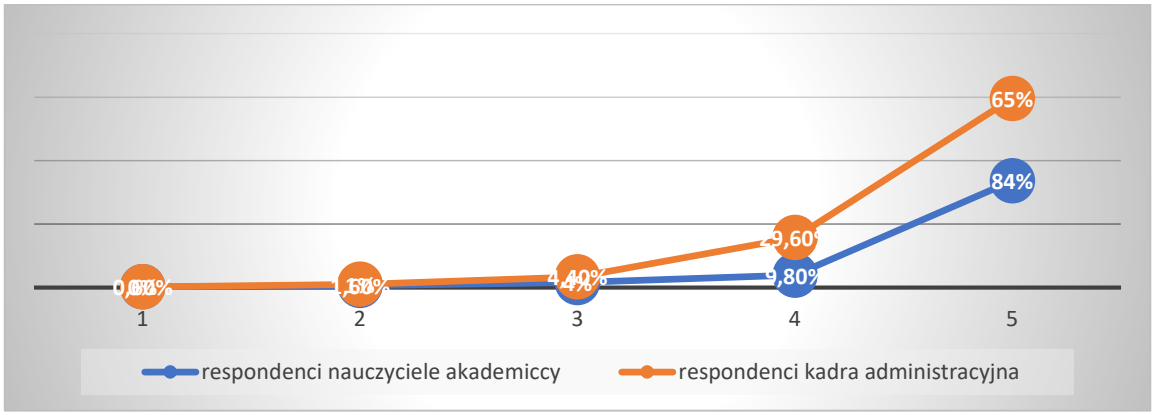
Źródło: opracowanie własne na podstawie badań własnych

Ogólna ocena średnia dla grupy nauczycieli akademickich wynosi 4,75%, zaś dla kadry administracyjnej wynosi 4,58%. Istnieje zależność między zmiennymi a świadczy o tym współczynnik korelacji liniowej Pearsona na poziomie 0,94 i współczynnik determinacji liniowej, wskazujący procent wyjaśnionej liniowo zmienności i jest równy 88,36%.

$$r_{xy} = \frac{\frac{1}{n}\sum_{i=1}^{n}(x_i-\bar{x})(y_i-\bar{y})}{S_x S_y}=0{,}94$$

$$\mathrm{WD}=r_{xy}^{2} * 100\% = 88{,}36\%$$

Wykres. 2.2. Zależności między respondentami, nauczycielami akademickimi i kadrą administracyjną pod względem najczęściej wykorzystywanego kanału do przekazywania informacji, jakim jest (wirtualna uczelnia i dziekanat10/USOS)



Źródło: opracowanie własne na podstawie badań własnych

Reasumując, rozkład badanych zmiennych wskazuje, że zarówno nauczyciele akademiccy jak i kadra administracyjna korzysta z kanałów wewnętrznych do szybkiego komunikowania się najczęściej ze studentami. Ten sposób przekazywania informacji jest bardzo sprawny, szybki i wygodny, ponieważ wiadomość może zostać wysłana do większej ilości osób poprzez zaznaczenie takiej opcji.

Tabela 2.2. przedstawia rozkład odpowiedzi na temat wykorzystania kanału do przekazywania informacji w uczelni wyższej, jakim jest (wirtualna uczelnia, dziekanat10/USOS).

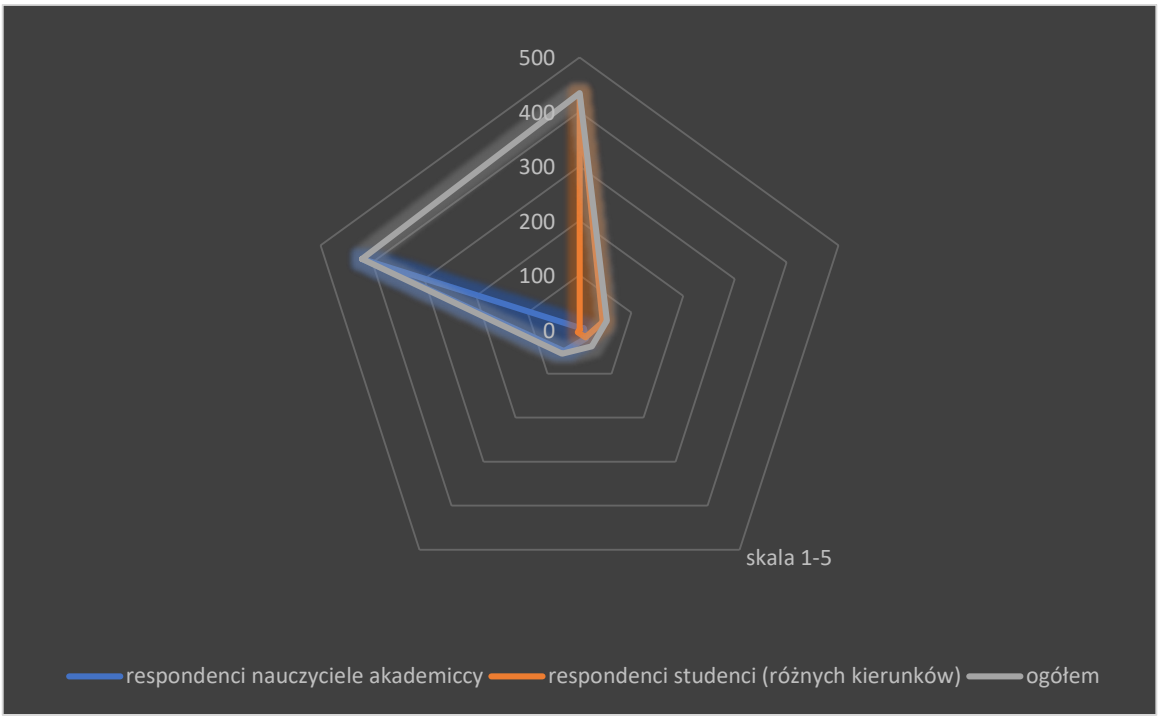
Tabela 2.2. Odpowiedzi respondentów grupy reprezentującej nauczycieli akademickich oraz grupy reprezentującej studentów (różnych kierunków) na temat najczęściej wykorzystywanego kanału przekazywania informacji, jakim jest (wirtualna uczelnia i dziekanat10/USOS)

Odpowiedzi badanych osób • **Zastosowany rodzaj kanału obiegu informacji (wirtualna uczelnia, dziekanat10/USOS)**									
Osoby poddane badaniu	**Respondenci nauczyciele akademiccy**			**Respondenci studenci (różne kierunki)**			**OGÓŁEM**		
Ocena od 1-5	***liczba wskazań***	***udział procentowy***	***ocena średnia***	***liczba wskazań***	***udział procentowy***	***ocena średnia***	***liczba wskazań***	***udział procentowy***	***ocena średnia***
1	3	0,6%	0,006	431	86,2%	0,86	434	43,4%	0,43
2	8	1,6%	0,03	45	9%	0,18	53	5,3%	0,11
3	20	4%	0,12	18	4%	0,12	38	3,8%	0,11
4	49	9,8%	0,39	6	1,2%	0,5	55	5,5%	0,22
5	420	84%	4,2	0	0,0	0	420	42%	2,1
	500	**100%**	**4,75**	**500**	**100%**	**1,66**	**1000**	**100%**	**2,97**

Źródło: Opracowanie własne na podstawie własnych badań

W badaniu wzięło udział 500 osób zatrudnionych na stanowisku, nauczycieli akademickich oraz 500 osób będących studentami uczelni wyższej. Wszystkie wyżej wskazane osoby poprawnie udzieliły odpowiedzi w ilości 100%. Nie doszło do sytuacji, w której odpowiedzi zostały błędnie wskazane. W przypadku nauczycieli akademickich najwyższą (najczęstszą) odpowiedź odnośnie kanału przekazywania informacji, jaką jest *wirtualna uczelnia, dziekanat10/USOS,* udzieliło 420 respondentów to jest 84%. Najniższą odpowiedź (najrzadziej) korzysta z tej drogi przekazu informacji 3 osoby to jest 0,6%. Studenci (różnych kierunków) zadeklarowali najwyższą (najczęstszą) drogę przesyłu informacji w ilości 0 respondentów, najniższą (najrzadszą) drogę dystrybucji informacji dla tej grupy zadeklarowało 431 respondentów to jest 86,2%.

Wykres 2.3. Odpowiedzi respondentów grupy nauczycieli akademickich i grupy studentów na temat najczęściej wykorzystanego kanału do przekazywania informacji, jakim jest (wirtualna uczelnia i dziekanat10/USOS)



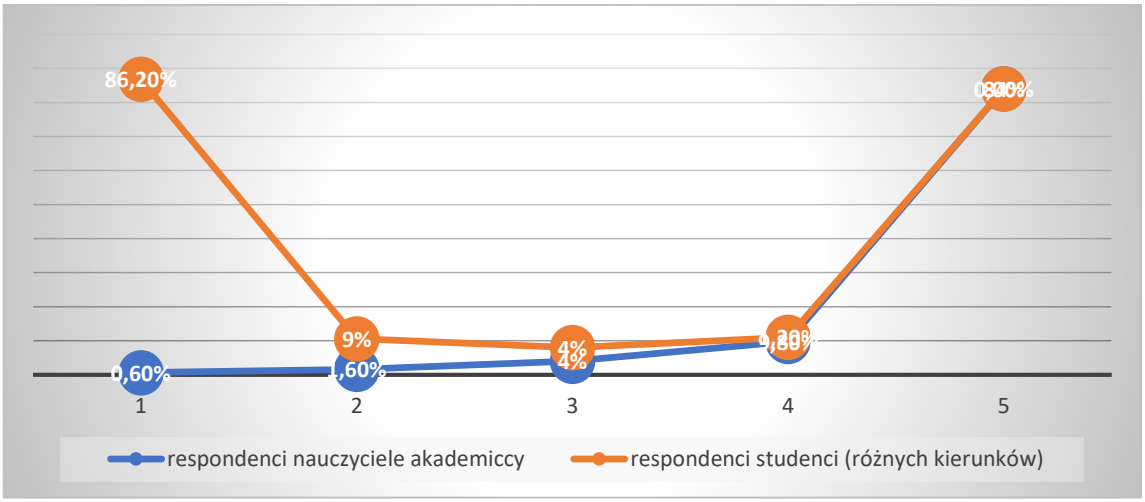
Źródło: opracowanie własne na podstawie badań własnych

Ogólna ocena średnia dla grupy nauczycieli akademickich wynosi 4,75%, zaś dla grupy studentów wynosi 2,97%. W przypadku tych dwóch grup widać, że wzrost wartości jednej zmiennej wiąże się ze spadkiem wartości drugiej zmiennej. Świadczy o tym współczynnik korelacji liniowej Pearsona na poziomie – 0,36 a współczynnik determinacji liniowej, wskazujący procent wyjaśnionej liniowo zmienności jest równy 12,96 %.

$$r_{xy} = \frac{\frac{1}{n}\sum_{i=1}^{n}(x_i-\bar{x})(y_i-\bar{y})}{S_x S_y}\text{=-0,36}$$

$$\text{WD=r}\frac{2}{xy} * 100\% = 12{,}96\%$$

Wykres 2.4. Zależności między respondentami, nauczycielami akademickimi i studentami pod względem najczęściej wykorzystywanego kanału do przekazywania informacji, jakim jest (wirtualna uczelnia, dziekanat10/USOS)



Źródło: opracowanie własne na podstawie badań własnych

Reasumując, rozkład badanych zmiennych wskazuje, że nauczyciele akademiccy w wyższym stopniu korzystają z tej ścieżki przekazywania informacji. Studenci wybiórczo wysyłają za pomocą wirtualnej uczelni, dziekanatu10 wszelkie informacje. Mimo szybkiego, sprawnego komunikowania przez ten węzeł przepływu informacji studenci wybierają inne źródła komunikacji. Tabela 2.3 przedstawia rozkład odpowiedzi na temat wykorzystania kanału do przekazywania informacji w uczelni wyższej, jakim jest (wirtualna uczelnia, dziekanat10/USOS).

Tabela 2.3. Odpowiedzi respondentów grupy kadra administracyjna i grupy studenci na temat najczęściej wykorzystywanego kanału do przekazywania informacji, jakim jest (wirtualna uczelnia, dziekanat10/USOS)

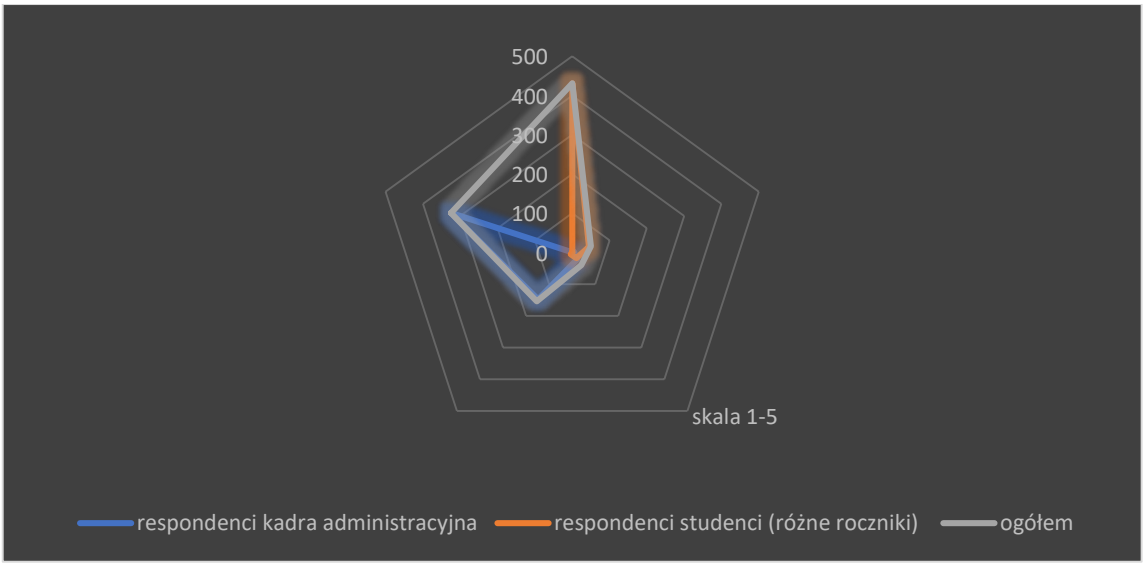
Odpowiedzi badanych osób • **Zastosowany rodzaj kanału obiegu informacji (wirtualna uczelnia, dziekanat10)**									
Osoby poddane badaniu	**Respondenci kadra administracyjna**			**Respondenci studenci (różne kierunki)**			**OGÓŁEM**		
Ocena od 1-5	***liczba wskazań***	***udział procentowy***	***ocena średnia***	***liczba wskazań***	***udział procentowy***	***ocena średnia***	***liczba wskazań***	***udział procentowy***	***ocena średnia***
1	0	0%	0,0	431	86,2%	0,86	431	43,1%	0,43
2	5	1%	0,02	45	9%	0,18	50	5%	0,1
3	22	4,4%	0,13	18	4%	0,12	40	4%	0,12
4	148	29,6%	1,18	6	1,2%	0,5	154	15,4%	0,62
5	325	65%	3,25	0	0,0	0	325	32,5%	1,62
	500	**100%**	**4,58**	**500**	**100%**	**1,66**	**1000**	**100%**	**2,89**

Źródło: opracowanie własne na podstawie badań własnych

W badaniu wzięło udział 500 osób zatrudnionych na stanowisku, kadry administracyjnej oraz 500 osób studiujących na uczelni wyższej. Wszystkie wyżej wskazane

osoby poprawnie udzieliły odpowiedzi w ilości 100%. Nie doszło do sytuacji, w której odpowiedzi zostały błędnie wskazane. W przypadku kadry administracyjnej najwyższą (najczęstszą) odpowiedź odnośnie kanału przekazywania informacji, jaką jest *wirtualna uczelnia, dziekanat10/USOS* udzieliło 325 respondentów to jest 65%. Nie ma osoby, która nie korzysta z tej ścieżki przekazu informacji. W przypadku studentów odpowiedź najwyższą nie zadeklarował żaden student, w związku z powyższym udział procentowy wynosił 0% a 431 respondentów studentów zadeklarowało, że rzadko korzysta z tej drogi dystrybucji informacji jest to 86,2%.

Wykres 2.5. Odpowiedzi respondentów grupy kadra administracyjna i grupy studenci na temat najczęściej wykorzystywanego kanału do przekazywania informacji, jakim jest (wirtualna uczelnia, dziekanat10/USOS



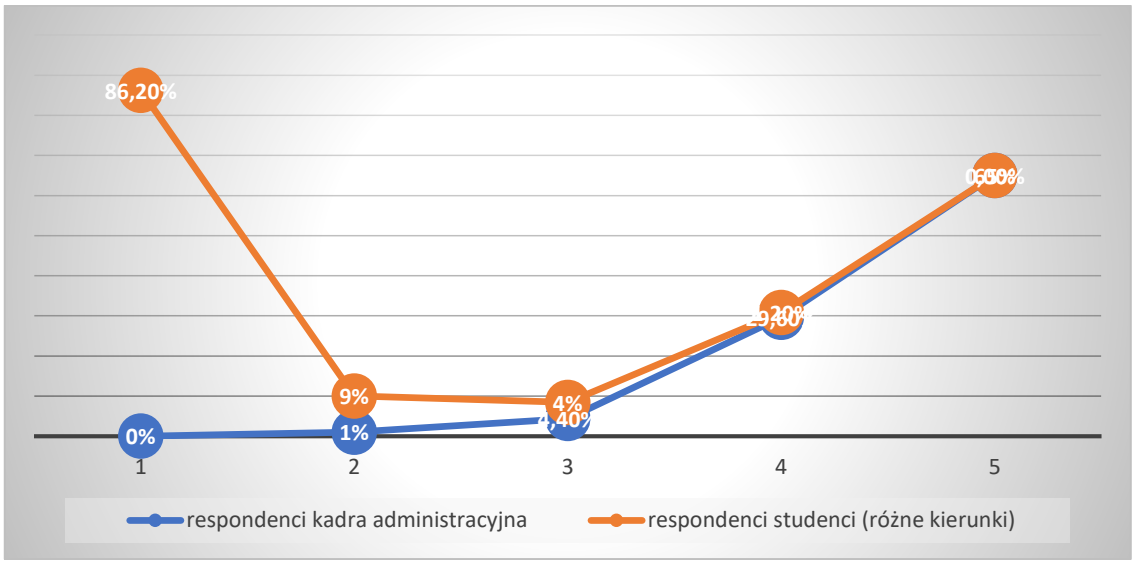
Źródło: opracowanie własne na podstawie badań własnych

Ogólna ocena średnia dla grupy kadry administracyjnej wynosi 4,58%, zaś dla grupy studentów wynosi 1,66%. Wzrost wartości jednej zmiennej wiąże się ze spadkiem wartości drugiej zmiennej a świadczy o tym współczynnik korelacji liniowej Pearsona na poziomie – 0,47 a współczynnik determinacji liniowej, wskazuje procent wyjaśnionej liniowo zmienności i jest równy 22,09 %.

$$r_{xy} = \frac{\frac{1}{n}\sum_{i=1}^{n}(x_i-\bar{x})(y_i-\bar{y})}{S_x S_y} = -0{,}47$$

$$\mathrm{WD} = r_{xy}^{2} * 100\% = 22{,}09\%$$

Wykres 2.6. Zależność między respondentami grupy kadry administracyjnej i grupy studentów pod względem najczęściej wykorzystywanego kanału do przekazywania informacji, jakim jest (wirtualna uczelnia, dziekanat10/USOS)



Źródło: opracowanie własne na podstawie badań własnych

W odniesieniu do analiz, rozkład badanych zmiennych wskazuje, że kadra administracyjna w wyższym stopniu częściej korzysta z tej ścieżki przekazywania informacji. Studenci wybiórczo wysyłają za pomocą wirtualnej uczelni, dziekanatu10 i USOS-a wszelkie informacje. Mimo szybkiego i sprawnego komunikowania przez ten węzeł przepływu informacji studenci wybierają inne źródła komunikacji.

1. W jaki sposób najczęściej Państwo przekazujecie i odbieracie informacje w uczelni wyższej?

b) Kanał obiegu informacji – informacje na piśmie

W całym badaniu wzięło udział 1500 respondentów, po 500 osób z każdej grupy (nauczyciele akademiccy, kadra administracyjna, studenci (różne kierunki).

W tabeli 2.4 zaprezentowano rozkład odpowiedzi na temat wykorzystanego w uczelni wyższej kanału obiegu informacji, jakim są informacje na piśmie. Zostały porównane 2 grupy respondentów nauczyciele akademiccy i grupy kadra administracyjna.

Tabela 2.4. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy kadra administracyjna na temat najczęściej wykorzystywanego kanału do przekazywania informacji, jakim są informacje na piśmie

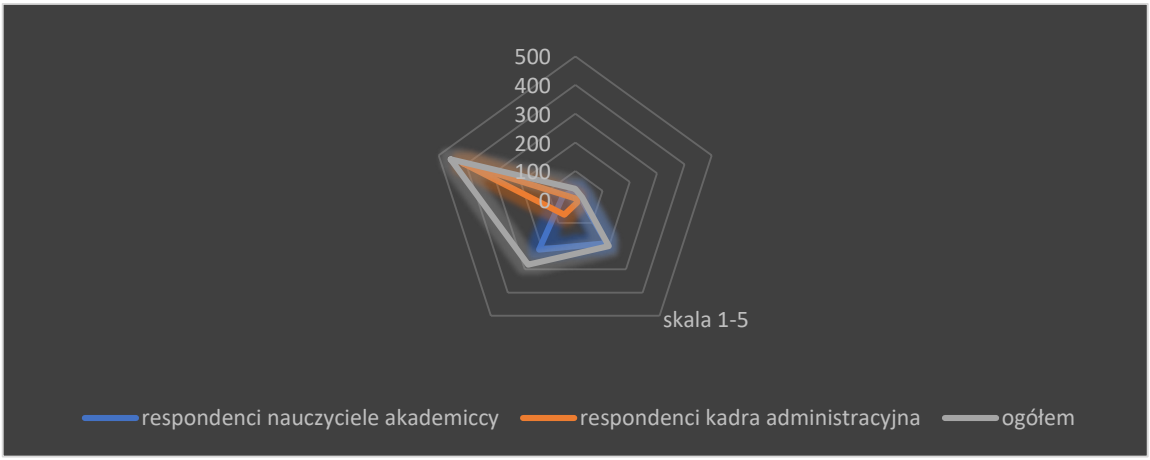
Odpowiedzi badanych osób • **Zastosowany rodzaj kanału obiegu informacji (na piśmie)**									
Osoby poddane badaniu	**Respondenci nauczyciele akademiccy**			**Respondenci kadra administracyjna**			**OGÓŁEM**		
Ocena od 1-5	***liczba wskazań***	***udział procentowy***	***ocena średnia***	***liczba wskazań***	***udział procentowy***	***ocena średnia***	***liczba wskazań***	***udział procentowy***	***ocena średnia***
1	33	6,6%	0,7	5	1%	0,01	38	3,8%	0,04
2	20	4%	0,08	6	1,2%	0,02	26	2,6%	0,05
3	187	37,4%	1,12	12	2,4%	0,07	199	19,9%	0,60
4	215	43%	1,72	65	13%	0,52	280	28%	1,12
5	45	9%	0,45	412	82,4%	4,12	457	45,7%	1,28
	500	**100%**	**4,07**	**500**	**100%**	**4,74**	**1000**	**100%**	**3,09**

Źródło: opracowanie własne na podstawie badań własnych

W badaniu wzięło udział 500 osób zatrudnionych na stanowisku, nauczycieli akademickich oraz 500 osób zatrudnionych na stanowisku kadry administracyjnej. Wszystkie wyżej wskazane osoby poprawnie udzieliły odpowiedzi w ilości 100%. Nie doszło do sytuacji, w której odpowiedzi zostały błędnie wskazane. W przypadku nauczycieli akademickich najwyższą (najczęstszą) odpowiedź odnośnie kanału przekazywania informacji, jaką są informacje przekazywane na piśmie udzieliło 45 respondentów to jest 9%. Najniższą odpowiedź (najrzadziej) korzysta z tej drogi przekazu informacji 33 osoby to jest 6,6%. Kadra administracyjna zadeklarowała najwyższą (najczęstszą) drogę przesyłu informacji w ilości 412 respondentów to jest 82,4%.

Liczba wskazań najniższej oceny (najrzadszej) dla kadry administracyjnej wynosiła 5 co w przeliczeniu procentowym daje 10%.

Wykres 2.7. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy kadra administracyjna na temat najczęściej wykorzystywanego kanału do przekazywania informacji, jakim są informacje na piśmie



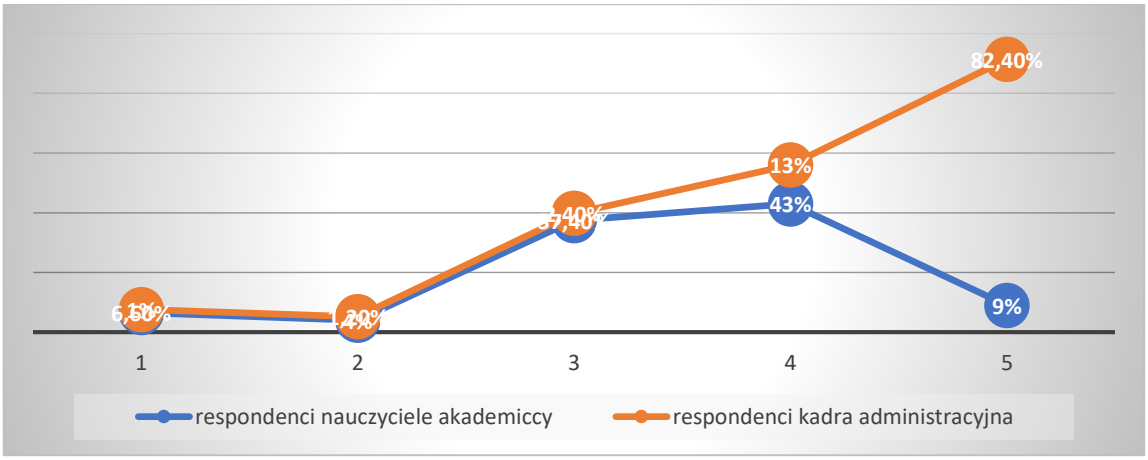
Źródło: opracowanie własne na podstawie badań własnych

Ogólna ocena średnia dla grupy nauczycieli akademickich wynosi 4,07%, zaś dla kadry administracyjnej wynosi 4,74%. Widać, że wzrost wartości jednej zmiennej wiąże się ze spadkiem wartości drugiej zmiennej a świadczy o tym współczynnik korelacji liniowej Pearsona na poziomie – 0,23 i współczynnik determinacji liniowej, wskazujący procent wyjaśnionej liniowo zmienności który jest równy 5,29%.

$$r_{xy} = \frac{\frac{1}{n}\sum_{i=1}^{n}(x_i-\bar{x})(y_i-\bar{y})}{S_x S_y}\text{=-0,23}$$

$$\text{WD=r}\frac{2}{xy} * 100\% = 5{,}29\%$$

Wykres 2.8. Zależność między respondentami grupy nauczyciele akademiccy i grupy kadra administracyjna pod względem najczęściej wykorzystywanego kanału do przekazywania informacji, jakim są informacje na piśmie



Źródło: opracowanie własne na podstawie badań własnych

Reasumując, rozkład badanych zmiennych wskazuje, że zarówno nauczyciele akademiccy jak i kadra administracyjna korzysta z kanałów przekazywania informacji, jakimi są informacje przekazywane na piśmie. Ten sposób dystrybucji informacji jest nieodzowny, jeżeli chodzi o jednostki administracji publicznej. W tabeli 2.5 został zaprezentowany rozkład odpowiedzi na temat wykorzystywania kanału do obiegu informacji w uczelni wyższej, jakim jest przekaz informacji na piśmie. Analizie zostały poddane grupy takie jak nauczyciele akademiccy oraz studenci (różne kierunki).

Tabela 2.5. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy studentów (różnych kierunków) na temat najczęściej wykorzystywanego kanału do przekazywania informacji, jakim są informacje na piśmie

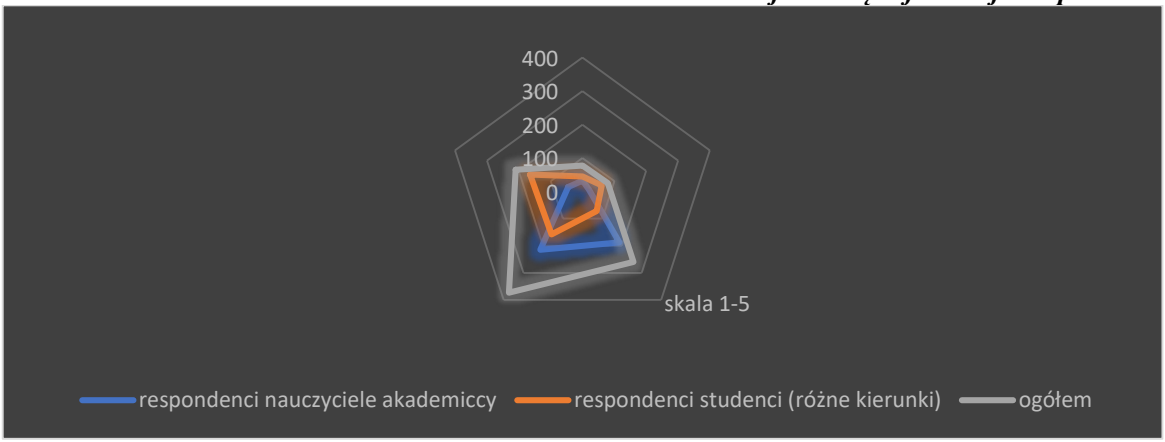
Odpowiedzi badanych osób • **Zastosowany rodzaj kanału obiegu informacji (na piśmie)**									
Osoby poddane badaniu	**Respondenci nauczyciele akademiccy**			**Respondenci studenci (różne kierunki)**			**OGÓŁEM**		
Ocena od 1-5	***liczba wskazań***	***udział procentowy***	***ocena średnia***	***liczba wskazań***	***udział procentowy***	***ocena średnia***	***liczba wskazań***	***udział procentowy***	***ocena średnia***
1	33	6,6%	0,7	45	9%	0,09	78	7,8%	0,08
2	20	4%	0,08	60	12%	0,24	80	8%	0,16
3	187	37,4%	1,12	72	14,4%	0,43	259	25,9%	0,78
4	215	43%	1,72	158	31,6%	1,26	373	37,3%	1,49
5	45	9%	0,45	165	33%	1,65	210	21%	1,05
	500	**100%**	**4,07**	**500**	**100%**	**3,67**	**1000**	**100%**	**3,56**

Źródło: opracowanie własne na podstawie badań własnych

W badaniu wzięło udział 500 osób zatrudnionych na stanowisku, nauczycieli akademickich oraz 500 osób studiujących w uczelni wyższej. Wszystkie wyżej wskazane osoby poprawnie udzieliły odpowiedzi w ilości 100%. Nie doszło do sytuacji, w której odpowiedzi zostały błędnie wskazane. W przypadku nauczycieli akademickich najwyższą (najczęstszą) odpowiedź odnośnie kanału przekazywania informacji, jaką są informacje udzielane na piśmie, udzieliło 45 respondentów to jest 9%.

Najniższą odpowiedź (najrzadziej) korzysta z tej drogi przekazu informacji 33 osoby to jest 6,6%. Studenci zadeklarowali najwyższą (najczęstszą) drogę przesyłu informacji w ilości 165 respondentów to jest 33%. Najniższą odpowiedź zadeklarowało 45 studentów to 9%.

Wykres 2.9. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy studenci na temat najczęściej wykorzystywanego kanału do przekazywania informacji, jakim są informacje na piśmie



Źródło: opracowanie własne na podstawie badań własnych

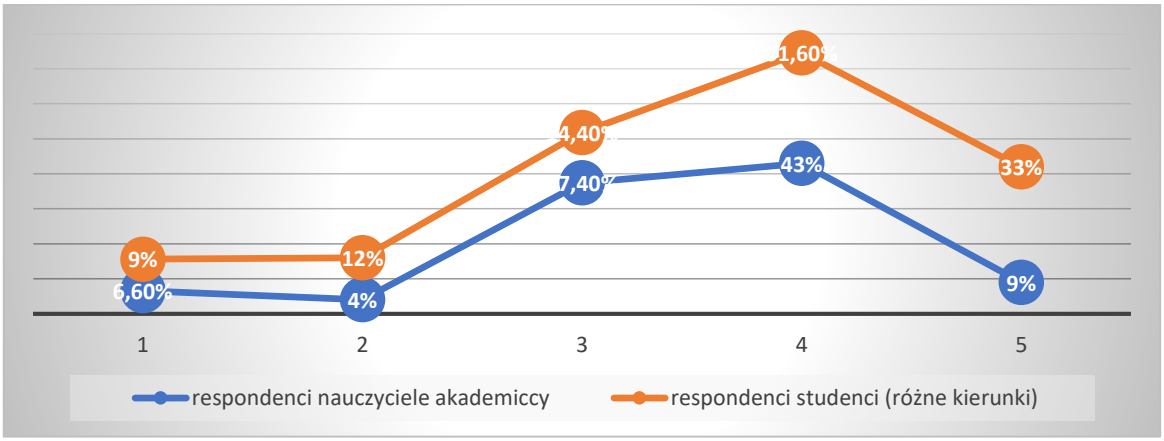
Ogólna ocena średnia dla grupy nauczycieli akademickich wynosi 4,07%, zaś dla grupy studentów wynosi 3,67%.

Istnieje zależność między zmiennymi a świadczy o tym współczynnik korelacji liniowej Pearsona na poziomie 0,35 i współczynnik determinacji liniowej, wskazujący procent wyjaśnionej liniowo zmienności i jest równy 12,25%.

$$r_{xy} = \frac{\frac{1}{n}\sum_{i=1}^{n}(x_i-\bar{x})(y_i-\bar{y})}{S_x S_y}=0{,}35$$

$$\text{WD}=r_{xy}^{2} * 100\% = 12{,}25\%$$

Wykres 2.10. Zależność między respondentami grupy nauczyciele akademiccy i grupy studenci pod względem najczęściej wykorzystywanego kanału do przekazywania informacji, jakim są informacje na piśmie



Źródło: opracowanie własne na podstawie badań własnych

Reasumując, rozkład badanych zmiennych wskazuje, że nauczyciele akademiccy częściej korzystają z kanałów przekazywania informacji w formie pisemnej. Studenci rzadziej korzystają z tej ścieżki przekazywania informacji jednakże nie jest to duża różnica pomiędzy jedną a drugą grupą badanych respondentów. Należy stwierdzić, że takie dokumenty na piśmie przekazywane są do wszystkich działów znajdujących się w uczelni wyższej, wewnętrznych do szybkiego komunikowania się najczęściej ze studentami. W tabeli 2.6. przedstawiono rozkład odpowiedzi respondentów należących do grupy kadry administracyjnej i grupy studentów z uwzględnieniem informacji na piśmie, jako kanału przekazu informacji w uczelni wyższej. Analizie zostały poddane grupy takie jak kadra administracyjna oraz studenci (różnych kierunków).

Tabela. 2.6. Odpowiedzi respondentów grupy kadra administracyjna i grupy studenci na temat najczęściej wykorzystywanego kanału do przekazywania informacji, jakim

Tabela. 2.6. Odpowiedzi respondentów grupy kadra administracyjna i grupy studenci na temat najczęściej wykorzystywanego kanału do przekazywania informacji, jakim są informacje na piśmie

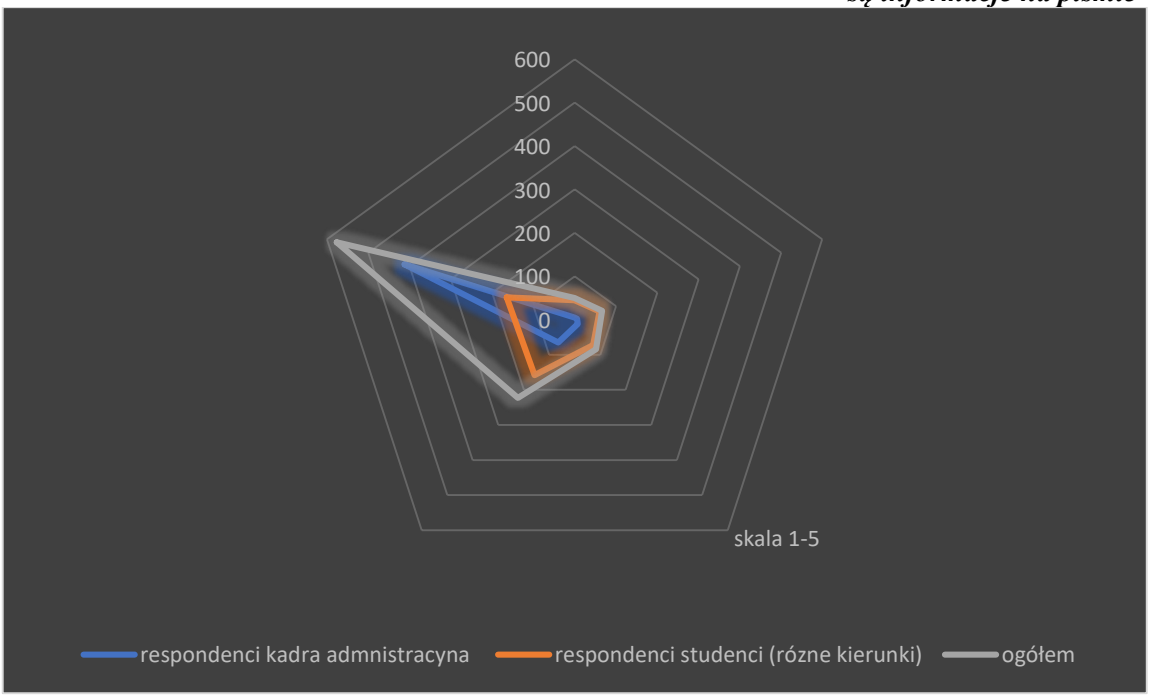
Odpowiedzi badanych osób • **Zastosowany rodzaj kanału obiegu informacji (na piśmie)**									
Osoby poddane badaniu	**Respondenci kadra administracyjna**			**Respondenci studenci (różne kierunki)**			**OGÓŁEM**		
Ocena od 1-5	***liczba wskazań***	***udział procentowy***	***ocena średnia***	***liczba wskazań***	***udział procentowy***	***ocena średnia***	***liczba wskazań***	***udział procentowy***	***ocena średnia***
1	5	1%	0,01	45	9%	0,09	50	5%	0,05
2	6	1,2%	0,02	60	12%	0,24	66	6,6%	0,13
3	12	2,4%	0,07	72	14,4%	0,43	84	8,4%	0,25
4	65	13%	0,52	158	31,6%	1,26	223	22,3%	0,89
5	412	82,4%	4,12	165	33%	1,65	577	57,7%	2,88
	500	**100%**	**4,74**	**500**	**100%**	**3,67**	**1000**	**100%**	**4,20**

Źródło: opracowanie własne na podstawie badań własnych

W badaniu wzięło udział 500 osób zatrudnionych na stanowisku, kadry administracyjnej oraz 500 osób studiujących na uczelni wyższej. Wszystkie wyżej wskazane osoby poprawnie udzieliły odpowiedzi w ilości 100%. Nie doszło do sytuacji, w której odpowiedzi zostały błędnie wskazane. W przypadku kadry administracyjnej najwyższą (najczęstszą) odpowiedź odnośnie kanału przekazywania informacji, jaką jest *informacja przekazywana na piśmie* udzieliło 412 respondentów to jest 82,4%. Najniższą odpowiedź (najrzadziej) korzysta z tej drogi przekazu informacji 5 osoby to jest 1%. Studenci zadeklarowali najwyższą (najczęstszą) drogę przesyłu informacji w ilości 165 respondentów

to jest 33%. Najrzadziej korzysta z tej formy przekazu informacji 45 respondentów z grupy studentów to jest 9%.

Wykres 2.11. Odpowiedzi respondentów pracowników administracyjnych i grupy studenci na temat najczęściej wykorzystywanego kanału do przekazywania informacji, jakim są informacje na piśmie



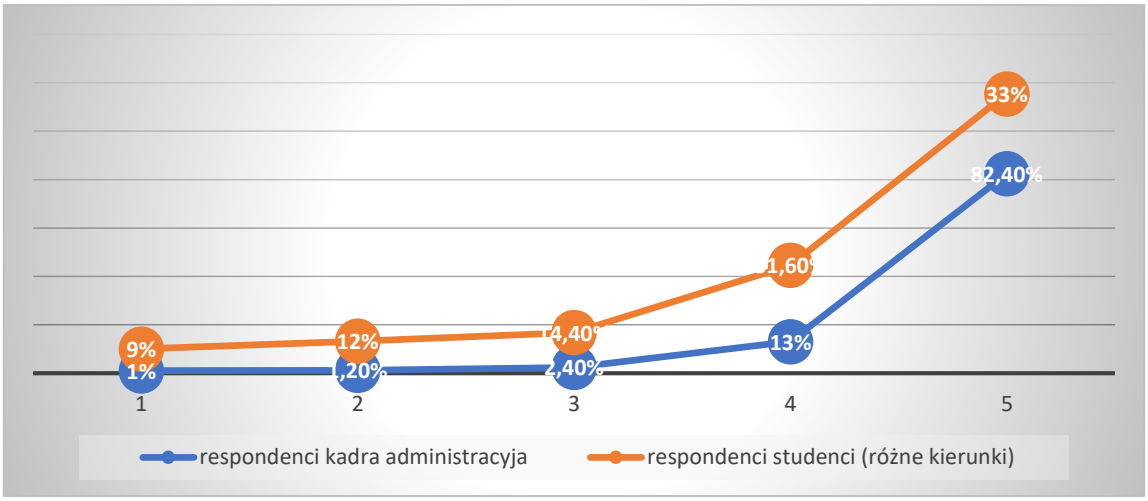
Źródło: opracowanie własne na podstawie badań własnych

Ogólna ocena średnia dla grupy kadra administracyjna wynosi 4,74%, zaś dla grupy studentów wynosi 3,67%. Istnieje zależność między zmiennymi a świadczy o tym współczynnik korelacji liniowej Pearsona na poziomie 0,74 i współczynnik determinacji liniowej, wskazujący procent wyjaśnionej liniowo zmienności i jest równy 54,76 %.

$$r_{xy} = \frac{\frac{1}{n}\sum_{i=1}^{n}(x_i-\bar{x})(y_i-\bar{y})}{S_x S_y}=0{,}74$$

$$\mathrm{WD}=r_{xy}^{2} * 100\% = 54{,}76\%$$

Wykres 2.12. Zależność między respondentami grupy kadra administracyjna i grupy studenci pod względem najczęściej wykorzystywanego kanału do przekazywania informacji, jakim są informacje na piśmie



Źródło: opracowanie własne na podstawie badań własnych

Reasumując, rozkład badanych zmiennych wskazuje, że kadra administracyjna bardzo często korzysta z tej formy przekazywania informacji. Studenci też korzystają z tej formy dystrybucji informacji jednakże w porównaniu z kadrą administracyjną ich potrzeba wymiany informacji w tej formie jest mniejsza.

1. W jaki sposób najczęściej Państwo przekazujecie i otrzymujecie informacje w uczelni wyższej?

c) Kanał obiegu informacji – przekaz ustny

W całym badaniu wzięło udział 1500 respondentów, po 500 osób z każdej grupy (nauczyciele akademiccy, kadra administracyjna, studenci (różne kierunki).

W tabeli 2.7 zaprezentowano rozkład odpowiedzi na temat wykorzystanego w uczelni wyższej kanału obiegu informacji, jakim jest przekaz ustny. Zostały porównane 2 grupy respondentów nauczyciele akademiccy i kadra administracyjna.

Tabela 2.7. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy kadra administracyjna na temat najczęściej wykorzystywanego kanału do przekazywania informacji, jakim jest przekaz ustny

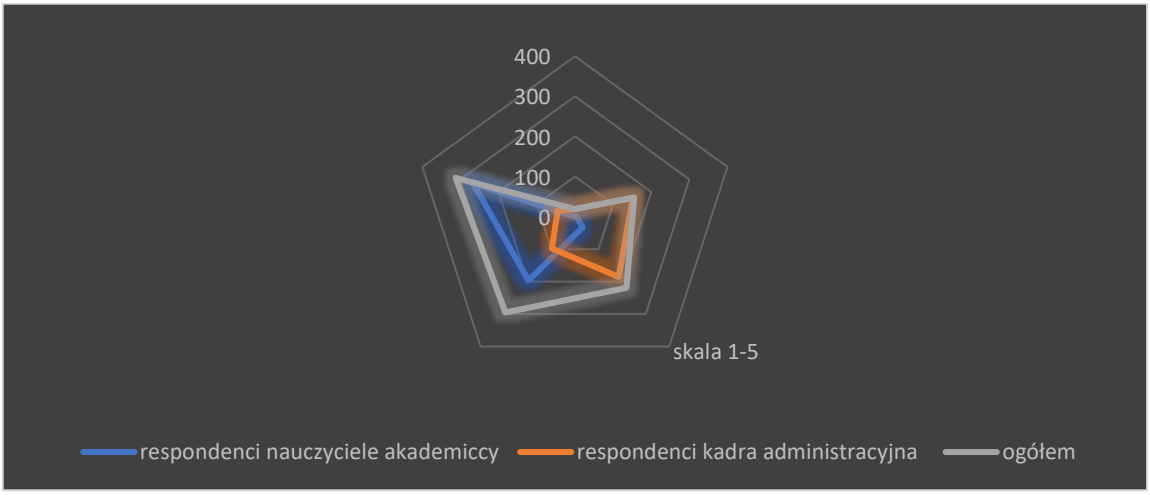
Odpowiedzi badanych osób • **Zastosowany rodzaj kanału obiegu informacji (przekaz ustny)**									
Osoby poddane badaniu	**Respondenci nauczyciele akademiccy**			**Respondenci kadra administracyjna**			**OGÓŁEM**		
Ocena od 1-5	***liczba wskazań***	***udział procentowy***	***ocena średnia***	***liczba wskazań***	***udział procentowy***	***ocena średnia***	***liczba wskazań***	***udział procentowy***	***ocena średnia***

1	0	0,0	0,0	19	3,8%	0,04	19	1,9%	0,2
2	3	0,6%	0,01	152	30,4%	0,61	155	15,5%	0,31
3	33	6,6%	0,20	186	37,2%	1,12	219	21,9%	0,66
4	197	39,4%	1,58	98	19,6%	0,78	295	29,5%	1,18
5	267	53,4%	2,67	45	9%	0,45	312	31,2%	1,56
	500	**100%**	**4,46**	**500**	**100%**	**3**	**1000**	**100%**	**3,91**

Źródło: opracowanie własne na podstawie badań własnych

W badaniu wzięło udział 500 osób zatrudnionych na stanowisku, nauczycieli akademickich oraz 500 osób zatrudnionych na stanowisku kadry administracyjnej. Wszystkie wyżej wskazane osoby poprawnie udzieliły odpowiedzi w ilości 100%. Nie doszło do sytuacji, w której odpowiedzi zostały błędnie wskazane. W przypadku nauczycieli akademickich najwyższą (najczęstszą) odpowiedź odnośnie kanału przekazywania informacji, jaką jest *przekaz ustny* udzieliło 267 respondentów to jest 53,4%. Nikt nie zadeklarował najniższej odpowiedzi (najrzadziej). Kadra administracyjna zadeklarowała najwyższą (najczęstszą) drogę przesyłu informacji w ilości 45 respondentów to jest 9%. Najrzadziej z tej formy przekazu informacji, jeżeli chodzi o kadrę administracyjną korzysta i zadeklarowało 19 respondentów to jest 3,8%.

Wykres 2.13. Odpowiedzi respondentów pracowników grupy nauczycieli akademickich i grupy kadry administracyjnej na temat najczęściej wykorzystywanego kanału do przekazywania informacji, jakim jest przekaz ustny



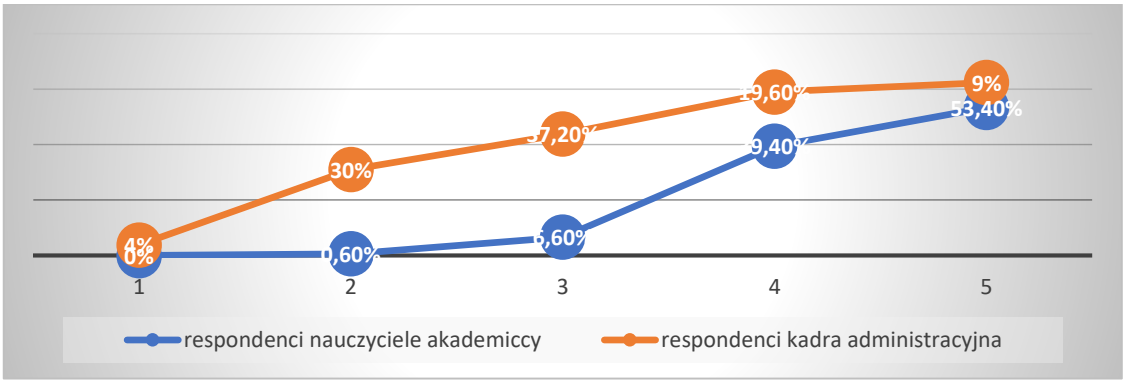
Źródło: opracowanie własne na podstawie badań własnych

Ogólna ocena średnia dla grupy nauczycieli akademickich wynosi 4,46%, zaś dla kadry administracyjnej wynosi 3%. W związku ze wzrostem wartości jednej zmiennej druga wartość spada, a świadczy o tym współczynnik korelacji liniowej Pearsona na poziomie -0,35 i współczynnik determinacji liniowej, wskazujący procent wyjaśnionej liniowo zmienności równy 12,25%.

$$r_{xy} = \frac{\frac{1}{n}\sum_{i=1}^{n}(x_i-\bar{x})(y_i-\bar{y})}{S_x S_y}$$=-0,35

$$\text{WD}=r_{xy}^{2} * 100\% = 12{,}25\%$$

Wykres 2.14. Zależność między respondentami grupy nauczycieli akademickich i grupy kadry administracyjnej pod względem najczęściej wykorzystywanego kanału do przekazywania informacji, jakim jest przekaz ustny



Źródło: opracowanie własne na podstawie badań własnych

Reasumując, rozkład badanych zmiennych wskazuje, że nauczyciele akademiccy często korzystają z formy przekazywania ustnie informacji, kadra administracyjna tą ścieżkę dosyć rzadko stosuje i może to być spowodowane koniecznością posiadania dokumentacji do ich dalszego procedowania. W tabeli 2.8 zaprezentowano rozkład odpowiedzi na temat wykorzystanego w uczelni wyższej kanału obiegu informacji, jakim jest przekaz ustny. Zostały porównane 2 grupy respondentów nauczyciele akademiccy i grupa studentów (różne roczniki).

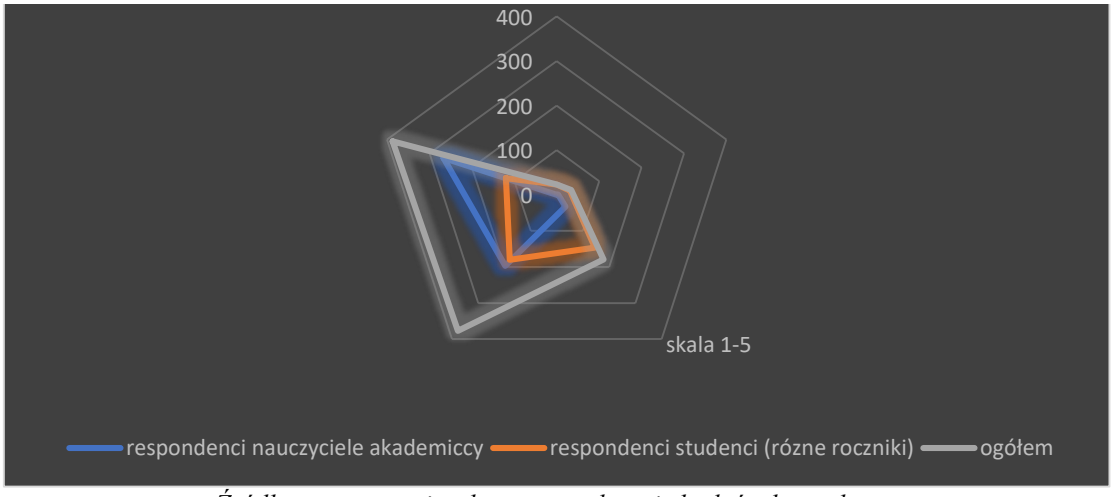
Tabela.2.8. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy studentów (różnych kierunków) na temat najczęściej wykorzystywanego kanału do przekazywania informacji, jakim jest przekaz ustny

Odpowiedzi badanych osób • **Zastosowany rodzaj kanału obiegu informacji (przekaz ustny)**									
Osoby poddane badaniu	**Respondenci nauczyciele akademiccy**			**Respondenci studenci (różne roczniki)**			**OGÓŁEM**		
Ocena od 1-5	***liczba wskazań***	***udział procentowy***	***ocena średnia***	***liczba wskazań***	***udział procentowy***	***ocena średnia***	***liczba wskazań***	***udział procentowy***	***ocena średnia***
1	0	0,0	0,0	23	4,6%	0,05%	23	2,3%	0,2
2	3	0,6%	0,01	31	6,2%	0,12%	34	3,4%	0,7
3	33	6,6%	0,20	146	29,2%	0,88%	179	17,9%	0,54
4	197	39,4%	1,58	180	36%	1,44%	377	37,7%	1,51
5	267	53,4%	2,67	120	24%	1,2%	387	38,7%	1,93
	500	**100%**	**4,46**	**500**	**100%**	**3,69**	**1000**	**100%**	**4,88**

Źródło: opracowanie własne na podstawie badań własnych

W badaniu wzięło udział 500 osób zatrudnionych na stanowisku, nauczycieli akademickich oraz 500 osób studiujących w uczelni wyższej. Wszystkie wyżej wskazane osoby poprawnie udzieliły odpowiedzi w ilości 100%. Nie doszło do sytuacji, w której odpowiedzi zostały błędnie wskazane. W przypadku nauczycieli akademickich najwyższą (najczęstszą) odpowiedź odnośnie kanału przekazywania informacji, jaką jest *przekaz ustny* udzieliło 267 respondentów to jest 53,4%. Nikt z nauczycieli akademickich nie zadeklarował najniższej (najrzadszej) drogi przekazu informacji w formie przekazu ustnego. Studenci zadeklarowali najwyższą odpowiedź w ilości 120 a to jest 24%. Najrzadziej korzysta z tej ścieżki przekazu informacji 23 studentów co daje 4,6%.

Wykres 2.15. Odpowiedzi respondentów pracowników grupy nauczycieli akademickich i grupy studentów (różnych roczników) na temat najczęściej wykorzystywanego kanału do przekazywania informacji, jakim jest przekaz ustny



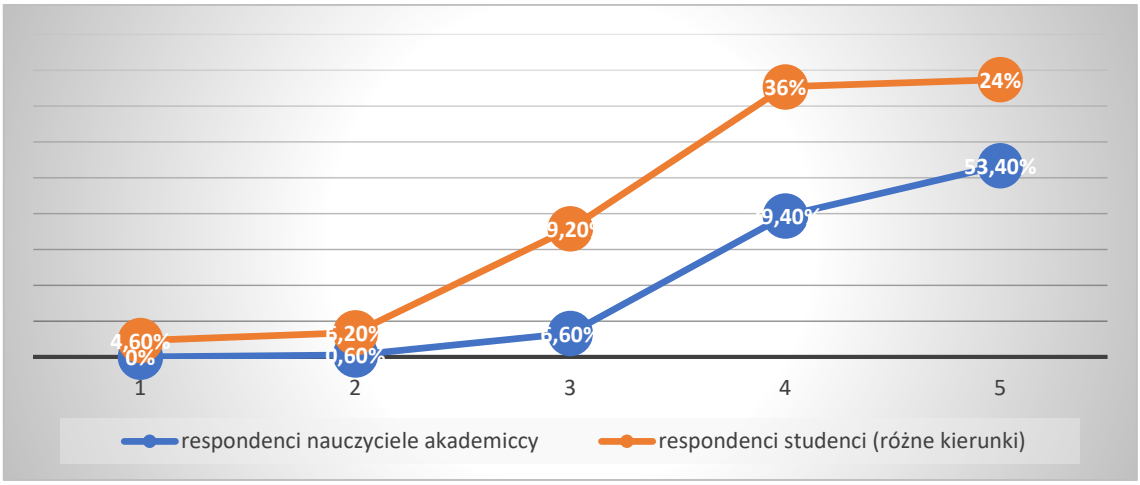
Źródło: opracowanie własne na podstawie badań własnych

Ogólna ocena średnia dla grupy nauczycieli akademickich wynosi 4,46%, zaś dla grupy studentów wynosi 3,67%. Istnieje zależność między zmiennymi a świadczy o tym współczynnik korelacji liniowej Pearsona na poziomie 0,65 i współczynnik determinacji liniowej, wskazujący procent wyjaśnionej liniowo zmienności i jest równy 42,25%.

$$r_{xy} = \frac{\frac{1}{n}\sum_{i=1}^{n}(x_i-\bar{x})(y_i-\bar{y})}{S_x S_y}=0{,}65$$

$$\mathrm{WD}=r\frac{2}{xy} * 100\% = 42{,}25\%$$

Wykres 2.16. Zależność między respondentami grupy nauczycieli akademickich i grupy studentów (różnych kierunków) pod względem najczęściej wykorzystywanego kanału do przekazywania informacji, jakim jest przekaz ustny



Źródło: opracowanie własne na podstawie badań własnych

Reasumując, rozkład badanych zmiennych wskazuje, że nauczyciele akademiccy w dużym stopniu korzystają z przekazu informacji w formie ustnej wypowiedzi. Wyniki analizy pokazują, ze studenci w mniejszym stopniu korzystają z tej formy przekazu informacji. W tabeli 2.9 zaprezentowano rozkład odpowiedzi na temat wykorzystanego w uczelni wyższej kanału obiegu informacji, jakim jest przekaz ustny. Zostały porównane 2 grupy respondentów kadra administracyjna i studenci (różnych kierunków).

Tabela 2.9. Odpowiedzi respondentów grupy kadra administracyjna i grupy studentów (różnych kierunków) na temat najczęściej wykorzystywanego kanału do przekazywania informacji, jakim jest przekaz ustny

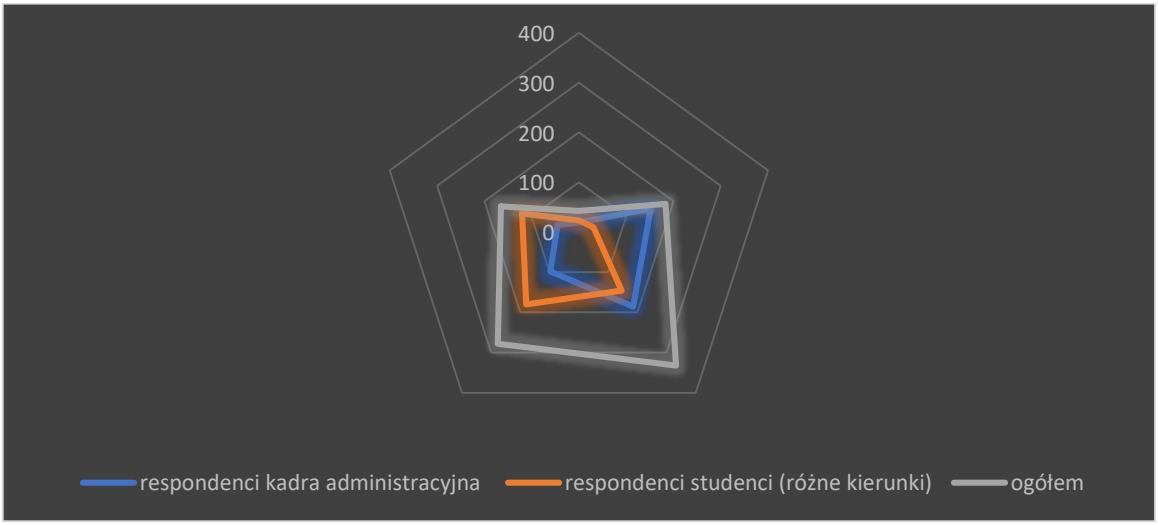
Odpowiedzi badanych osób • **Zastosowany rodzaj kanału obiegu informacji (przekaz ustny)**									
Osoby poddane badaniu	**Respondenci kadra administracyjna**			**Respondenci studenci (różne roczniki)**			**OGÓŁEM**		
Ocena od 1-5	***liczba wskazań***	***udział procentowy***	***ocena średnia***	***liczba wskazań***	***udział procentowy***	***ocena średnia***	***liczba wskazań***	***udział procentowy***	***ocena średnia***
1	19	3,8%	0,04	23	4,6%	0,05%	42	4,2%	0,04
2	152	30,4%	0,61	31	6,2%	0,12%	183	18,3%	0,37
3	186	37,2%	1,12	146	29,2%	0,88%	332	33,2%	1,0
4	98	19,6%	0,78	180	36%	1,44%	278	27,8%	1,11
5	45	9%	0,45	120	24%	1,2%	165	16,5%	0,82
	500	**100%**	**3**	**500**	**100%**	**3,69**	**1000**	**100%**	**3,34**

Źródło: opracowanie własne na podstawie badań własnych

W badaniu wzięło udział 500 osób zatrudnionych na stanowisku, kadry administracyjnej oraz 500 osób studiujących na uczelni wyższej. Wszystkie wyżej wskazane osoby poprawnie udzieliły odpowiedzi w ilości 100%. Nie doszło do sytuacji, w której

odpowiedzi zostały błędnie wskazane. W przypadku kadry administracyjnej najwyższą (najczęstszą) odpowiedź odnośnie kanału przekazywania informacji, jaką jest *przekaz ustny* udzieliło 45 respondentów to jest 9%. Najniższą odpowiedź (najrzadziej) korzysta z tej drogi przekazu informacji 19 osób to jest 3,8%. Studenci zadeklarowali najwyższą (najczęstszą) drogę przesyłu informacji w ilości 120 respondentów to jest 24%. Liczba wskazań dla odpowiedzi (najrzadziej) udzieliło 23 studentów to jest 4,6%.

Wykres 2.17. Odpowiedzi respondentów pracowników grupy kadra administracyjna i grupy studentów (różnych roczników) na temat najczęściej wykorzystywanego kanału do przekazywania informacji, jakim jest przekaz ustny



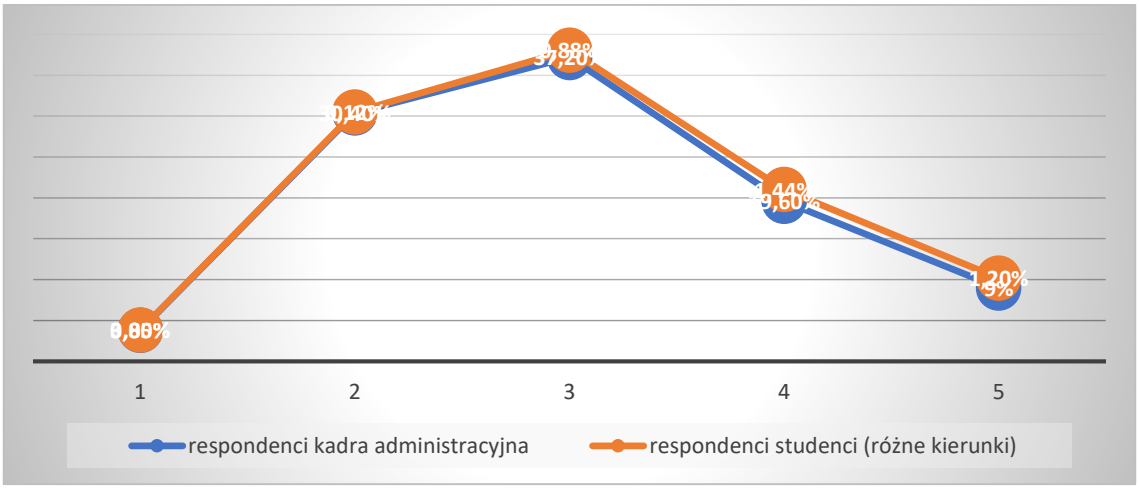
Źródło: opracowanie własne na podstawie badań własnych

Ogólna ocena średnia dla grupy kadry administracyjnej wynosi 3%, zaś dla grupy studentów wynosi 3,69%. Istnieje zależność między zmiennymi a świadczy o tym współczynnik korelacji liniowej Pearsona na poziomie 0,27 i współczynnik determinacji liniowej, wskazujący procent wyjaśnionej liniowo zmienności jest równy 7,29%.

$$r_{xy} = \frac{\frac{1}{n}\sum_{i=1}^{n}(x_i-\bar{x})(y_i-\bar{y})}{S_x S_y}=0{,}27$$

$$\mathrm{WD}=r_{xy}^{2} * 100\% = 7{,}29\%$$

Wykres 2.18. Zależność między respondentami grupy kadry administracyjnej i grupy studentów (różnych kierunków) pod względem najczęściej wykorzystywanego kanału do przekazywania informacji, jakim jest przekaz ustny



Źródło: opracowanie własne na podstawie badań własnych

1. W jaki sposób najczęściej Państwo przekazujecie i otrzymujecie informacje w uczelni wyższej?

d) Kanał obiegu informacji – poczta elektroniczna

W całym badaniu wzięło udział 1500 respondentów, po 500 osób z każdej grupy (nauczyciele akademiccy, kadra administracyjna, studenci (różne kierunki). W tabeli 2.10 zaprezentowano rozkład odpowiedzi na temat wykorzystanego w uczelni wyższej kanału obiegu informacji, jakim jest poczta elektroniczna. Zostały porównane 2 grupy respondentów nauczyciele akademiccy i kadra administracyjna.

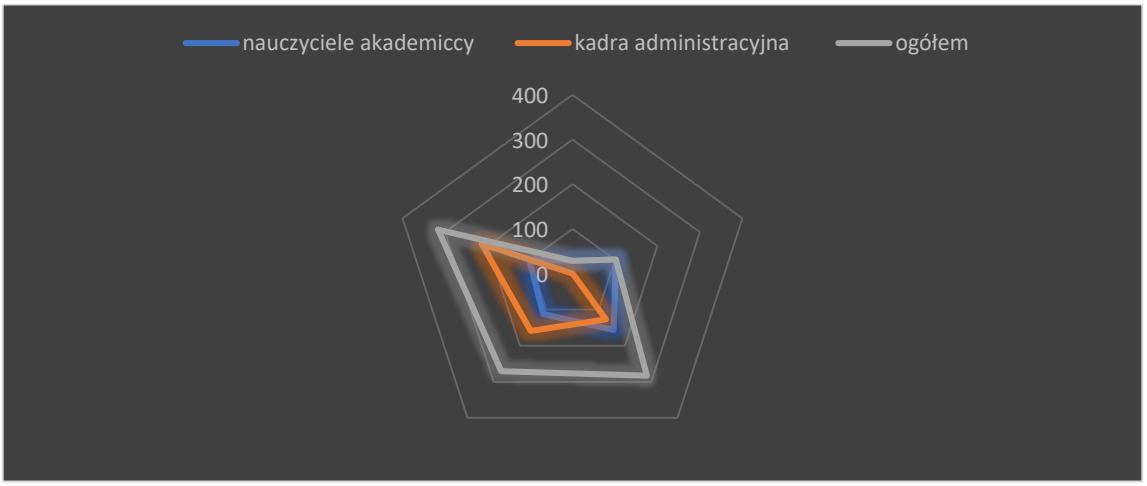
Tabela 2.10. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy kadra administracyjna na temat najczęściej wykorzystywanego kanału do przekazywania informacji, jakim jest poczta elektroniczna

Odpowiedzi badanych osób • **Zastosowany rodzaj kanału obiegu informacji (poczta elektroniczna)**									
Osoby poddane badaniu	**Respondenci nauczyciele akademiccy**			**Respondenci kadra administracyjna**			**OGÓŁEM**		
Ocena od 1-5	***liczba wskazań***	***udział procen-towy***	***ocena średnia***	***liczba wskazań***	***udział procen-towy***	***ocena średnia***	***liczba wskazań***	***udział procen-towy***	***ocena średnia***
1	28	5,6%	0,6	0	0,0%	0,0	28	2,8%	0,03
2	102	20,4%	0,41	0	0,0%	0,0	102	10,2%	0,20
3	156	31,2%	0,94	127	25,4%	0,76	283	28,3%	0,85
4	112	22,4%	0,90	159	31,8%	1,27	271	27,1%	1,08
5	102	20,4%	1,02	214	42,8%	2,14	316	31,6%	1,58
	500	**100%**	**3,87**	**500**	**100%**	**4,17**	**1000**	**100%**	**3,74**

Źródło: opracowanie własne na podstawie badań własnych

W badaniu wzięło udział 500 osób zatrudnionych na stanowisku, nauczycieli akademickich oraz 500 osób zatrudnionych na stanowisku kadry administracyjnej. Wszystkie wyżej wskazane osoby poprawnie udzieliły odpowiedzi w ilości 100%. Nie doszło do sytuacji, w której odpowiedzi zostały błędnie wskazane. W przypadku nauczycieli akademickich najwyższą (najczęstszą) odpowiedź odnośnie kanału przekazywania informacji, jaką jest *poczta elektroniczna* udzieliło 102 respondentów to jest 20,4%. Najniższą odpowiedź (najrzadziej) korzysta z tej drogi przekazu informacji 28 osób to jest 5,6 udziału procentowego. Kadra administracyjna zadeklarowała najwyższą (najczęstszą) drogę przesyłu informacji w ilości 214 respondentów to jest 42,8%. Jeżeli chodzi o najniższą odpowiedź (najrzadszą) to z kadry administracyjnej nikt nie zadeklarował takiej odpowiedzi i udział procentowy wynosił 0.

Wykres 2.19. Odpowiedzi respondentów pracowników grupy nauczyciele akademiccy i grupy kadra administracyjna na temat najczęściej wykorzystywanego kanału do przekazywania informacji, jakim jest poczta elektroniczna



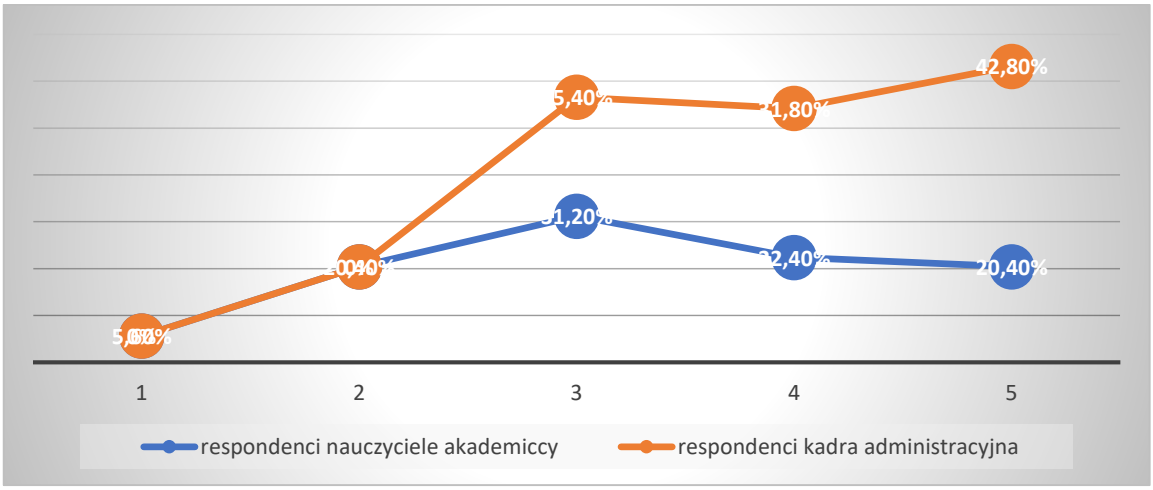
Źródło: opracowanie własne na podstawie badań własnych

Ogólna ocena średnia dla grupy nauczycieli akademickich wynosi 3,87%, zaś dla kadry administracyjnej wynosi 4,17%. Istnieje zależność między zmiennymi a świadczy o tym współczynnik korelacji liniowej Pearsona na poziomie 0,53 i współczynnik determinacji liniowej, wskazujący procent wyjaśnionej liniowo zmienności i jest równy 28,30%.

$$r_{xy} = \frac{\frac{1}{n}\sum_{i=1}^{n}(x_i-\bar{x})(y_i-\bar{y})}{S_x S_y}=0{,}53$$

$$\mathrm{WD}=r_{xy}^{2} * 100\% = 28{,}30\%$$

Wykres 2.20. Zależność między respondentami grupy nauczycieli akademickich i grupy kadry administracyjnej pod względem najczęściej wykorzystywanego kanału do przekazywania informacji, jakim jest poczta elektroniczna



Źródło: opracowanie własne na podstawie badań własnych

Reasumując, rozkład badanych zmiennych wskazuje, że nauczyciele akademiccy w mniejszym stopniu korzystają z kanału przekazywania informacji, jakim jest poczta elektroniczna w odwołaniu do kadry administracyjnej. Tam więcej respondentów zadeklarowało ten sposób komunikowania. W tabeli 2.11 zaprezentowano rozkład odpowiedzi na temat wykorzystanego w uczelni wyższej kanału obiegu informacji, jakim jest poczta elektroniczna. Zostały porównane 2 grupy respondentów nauczyciele akademiccy i studenci (różne roczniki).

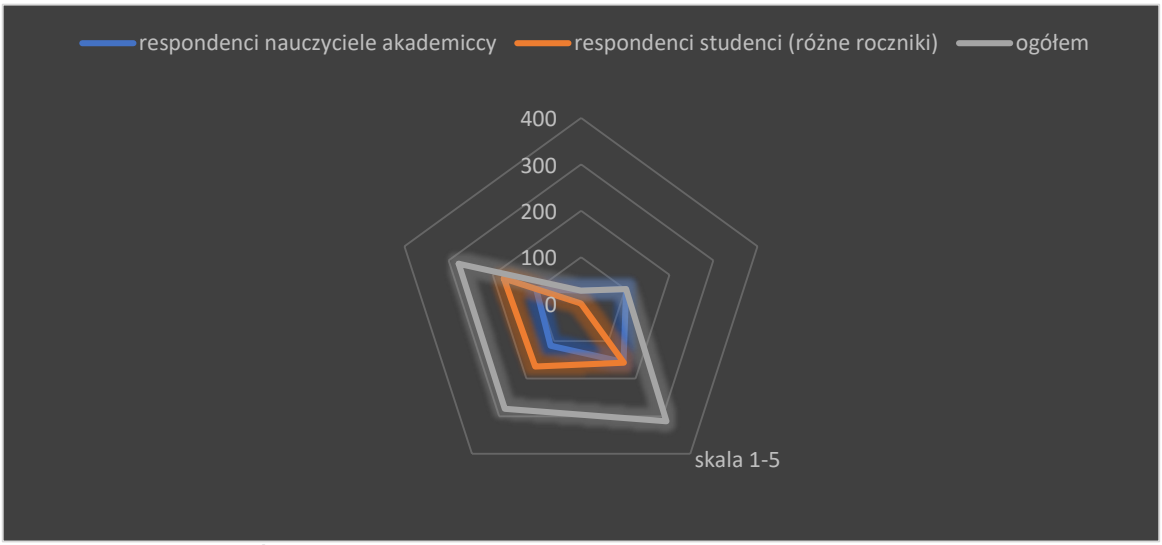
Tabela 2.11. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy studenci (różne roczniki) na temat najczęściej wykorzystywanego kanału do przekazywania informacji, jakim jest poczta elektroniczna

Odpowiedzi badanych osób • **Zastosowany rodzaj kanału obiegu informacji (poczta elektroniczna)**									
Osoby poddane badaniu	**Respondenci nauczyciele akademiccy**			**Respondenci studenci (różne kierunki)**			**OGÓŁEM**		
Ocena od 1-5	***liczba wskazań***	***udział procentowy***	***ocena średnia***	***liczba wskazań***	***udział procentowy***	***ocena średnia***	***liczba wskazań***	***udział procentowy***	***ocena średnia***
1	28	5,6%	0,6	0	0,0%	0,0	28	2,8%	0,03
2	102	20,4%	0,41	0	0,0%	0,0	102	10,2%	0,20
3	156	31,2%	0,94	157	31,4%	0,94	313	31,3%	0,94
4	112	22,4%	0,90	168	33,6%	1,34	280	28%	1,12
5	102	20,4%	1,02	175	35%	1,75	277	27%	1,35
	500	**100%**	**3,87**	**500**	**100%**	**4,03**	**1000**	**100%**	**3,64**

Źródło: opracowanie własne na podstawie badań własnych

W badaniu wzięło udział 500 osób zatrudnionych na stanowisku, nauczycieli akademickich oraz 500 studentów uczących się w uczelni wyższej. Wszystkie wyżej wskazane osoby poprawnie udzieliły odpowiedzi w ilości 100%. Nie doszło do sytuacji, w której odpowiedzi zostały błędnie wskazane. W przypadku nauczycieli akademickich najwyższą (najczęstszą) odpowiedź odnośnie kanału przekazywania informacji, jaką jest *poczta elektroniczna* udzieliło 102 respondentów to jest 20,4 udziału procentowego. Najniższą odpowiedź (najrzadziej) korzysta z tej drogi przekazu informacji 28 osób to jest 5,6 udziału procentowego. Studenci zadeklarowali najwyższą (najczęstszą) drogę przesyłu informacji w ilości 175 respondentów to jest 35 udziału procentowego. Liczba wskazań dla odpowiedzi najniższej (najrzadziej) dla grupy studentów wynosiła 0.

Wykres 2.21. Odpowiedzi respondentów pracowników grupy nauczyciele akademiccy i grupy studenci (różnych roczników) na temat najczęściej wykorzystywanego kanału do przekazywania informacji, jakim jest poczta elektroniczna



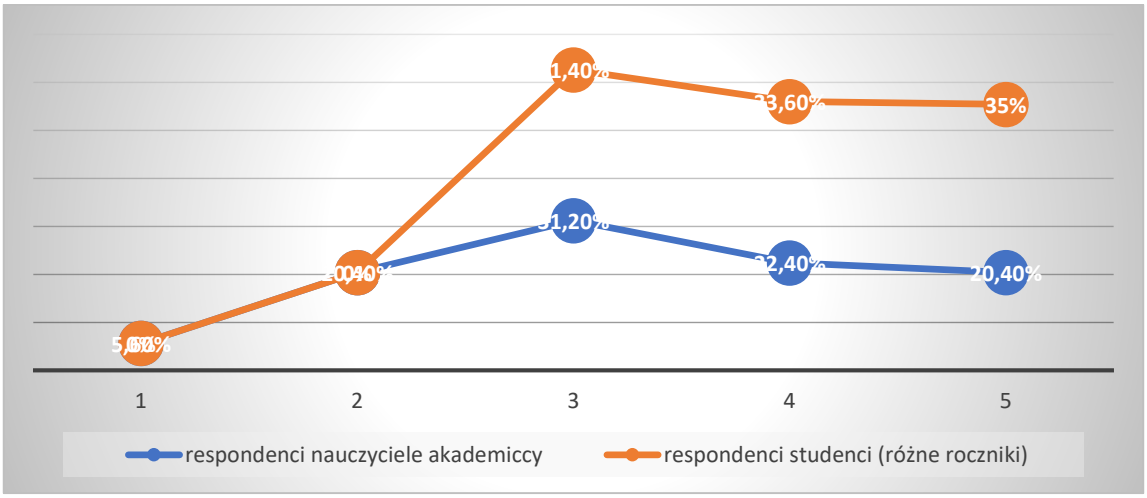
Źródło: opracowanie własne na podstawie badań własnych

Ogólna ocena średnia dla grupy nauczycieli akademickich wynosi 3,87%, zaś dla grupy studentów wynosi 4,03%. Istnieje zależność między zmiennymi a świadczy o tym współczynnik korelacji liniowej Pearsona na poziomie 0,66 i współczynnik determinacji liniowej, wskazujący procent wyjaśnionej liniowo zmienności i jest równy 43,56%.

$$r_{xy} = \frac{\frac{1}{n}\sum_{i=1}^{n}(x_i-\bar{x})(y_i-\bar{y})}{S_x S_y}=0{,}66$$

$$\mathrm{WD}=\mathrm{r}\frac{2}{xy} * 100\% = 43{,}56\%$$

Wykres 2.22. Zależność między respondentami grupy nauczycieli akademickich i grupy studentów (różne roczniki) pod względem najczęściej wykorzystywanego kanału do przekazywania informacji, jakim jest poczta elektroniczna



Źródło: opracowanie własne na podstawie badań własnych

Reasumując, rozkład badanych zmiennych wskazuje, że zarówno nauczyciele akademiccy jak i studenci korzystają z kanałów takich jak poczta elektroniczna. Funkcji wewnętrznych do szybkiego komunikowania się najczęściej ze studentami. Ten sposób przekazywania informacji jest bardzo sprawny, szybki i wygodny dla obydwóch stron zarówno nauczycieli akademickich jak i studentów. W tabeli 2.12 zaprezentowano rozkład odpowiedzi na temat wykorzystanego w uczelni wyższej kanału obiegu informacji, jakim jest poczta elektroniczna. Zostały porównane 2 grupy respondentów kadra administracyjna i studenci (różne roczniki).

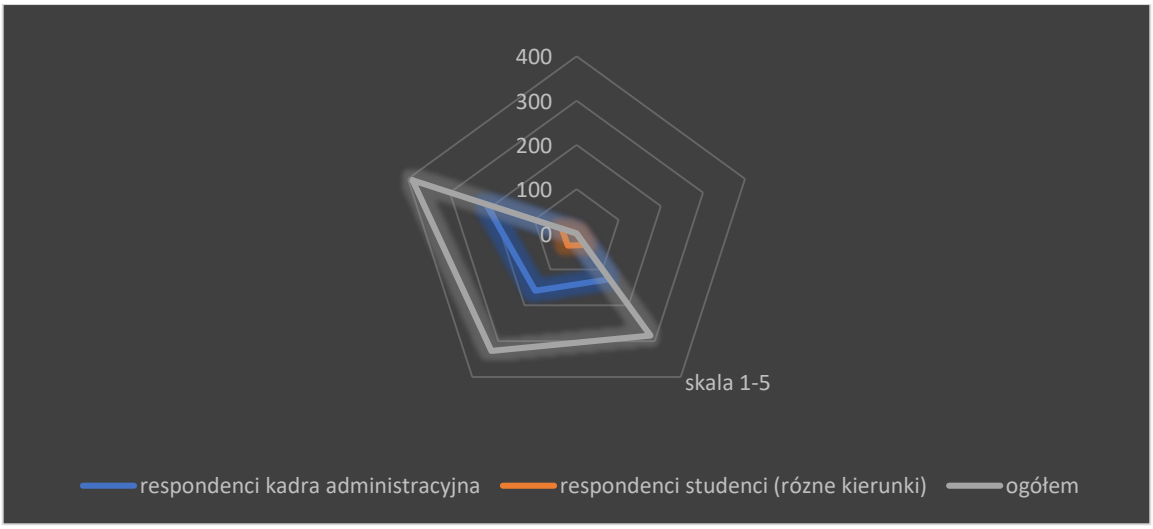
Tabela 2.12. Odpowiedzi respondentów grupy kadra administracyjna i grupy studenci (różne roczniki) na temat najczęściej wykorzystywanego kanału do przekazywania informacji, jakim jest poczta elektroniczna

Odpowiedzi badanych osób • **Zastosowany rodzaj kanału obiegu informacji (poczta elektroniczna)**									
Osoby poddane badaniu	**Respondenci kadra administracyjna**			**Respondenci studenci (różne kierunki)**			**OGÓŁEM**		
Ocena od 1-5	***liczba wskazań***	***udział procentowy***	***ocena średnia***	***liczba wskazań***	***udział procentowy***	***ocena średnia***	***liczba wskazań***	***udział procentowy***	***ocena średnia***
1	0	0,0%	0,0	0	0,0%	0,0	0	0,0%	0
2	0	0,0%	0,0	0	0,0%	0,0	0	0,0%	0
3	127	25,4%	0,76	157	31,4%	0,94	284	28,4%	0,85
4	159	31,8%	1,27	168	33,6%	1,34	327	32,7%	1,31
5	214	42,8%	2,14	175	35%	1,75	389	38,9%	1,94
	500	**100%**	**4,17**	**500**	**100%**	**4,03**	**1000**	**100%**	**4,10**

Źródło: opracowanie własne na podstawie badań własnych

W badaniu wzięło udział 500 osób zatrudnionych na stanowisku, kadry administracyjnej oraz 500 osób studiujących w uczelni wyższej. Wszystkie wyżej wskazane osoby poprawnie udzieliły odpowiedzi w ilości 100%. Nie doszło do sytuacji, w której odpowiedzi zostały błędnie wskazane. W przypadku kadry administracyjnej najwyższą (najczęstszą) odpowiedź odnośnie kanału przekazywania informacji, jaką jest *poczta elektroniczna* udzieliło 214 respondentów to jest 42,%. Najniższą odpowiedź (najrzadziej), jeżeli chodzi o kadrę administracyjną nikt z respondentów takiej odpowiedzi nie zadeklarował. Studenci, zaś zadeklarowali najwyższą (najczęstszą) drogę przesyłu informacji w ilości 175 respondentów to jest 35%.

Wykres 2.23. Odpowiedzi respondentów pracowników kadra administracyjna i grupy studenci (różnych roczników) na temat najczęściej wykorzystywanego kanału do przekazywania informacji, jakim jest poczta elektroniczna



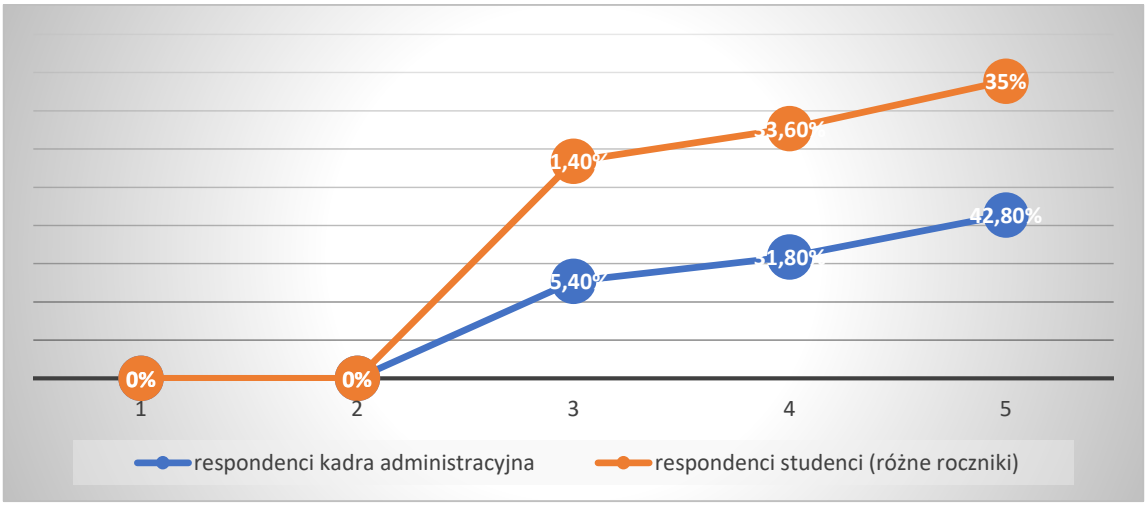
Źródło: opracowanie własne na podstawie badań własnych

Ogólna ocena średnia dla grupy kadry administracyjnej wynosi 4,17%, zaś dla grupy studentów wynosi 4,03%. Istnieje zależność między zmiennymi a świadczy o tym współczynnik korelacji liniowej Pearsona na poziomie 0,97 i współczynnik determinacji liniowej, wskazujący procent wyjaśnionej liniowo zmienności i jest równy 94,09%.

$$r_{xy} = \frac{\frac{1}{n}\sum_{i=1}^{n}(x_i-\bar{x})(y_i-\bar{y})}{S_x S_y}=0{,}97$$

$$\mathrm{WD}=r_{xy}^{2} * 100\% = 94{,}09\%$$

Wykres 2.24. Zależność między respondentami grupy kadra administracyjna i grupy studentów (różne roczniki) pod względem najczęściej wykorzystywanego kanału do przekazywania informacji, jakim jest poczta elektroniczna



Źródło: opracowanie własne na podstawie badań własnych

1. W jaki sposób najczęściej Państwo przekazujecie i otrzymujecie informacje w uczelni wyższej?

e) Kanał obiegu informacji – Aplikacja MsTeams

W całym badaniu wzięło udział 1500 respondentów, po 500 osób z każdej grupy (nauczyciele akademiccy, kadra administracyjna, studenci (różne kierunki). W tabeli 2.13 zaprezentowano rozkład odpowiedzi na temat wykorzystanego w uczelni wyższej kanału obiegu informacji, jakim jest aplikacja MsTeams. Zostały porównane 2 grupy respondentów nauczyciele akademiccy i kadra administracyjna.

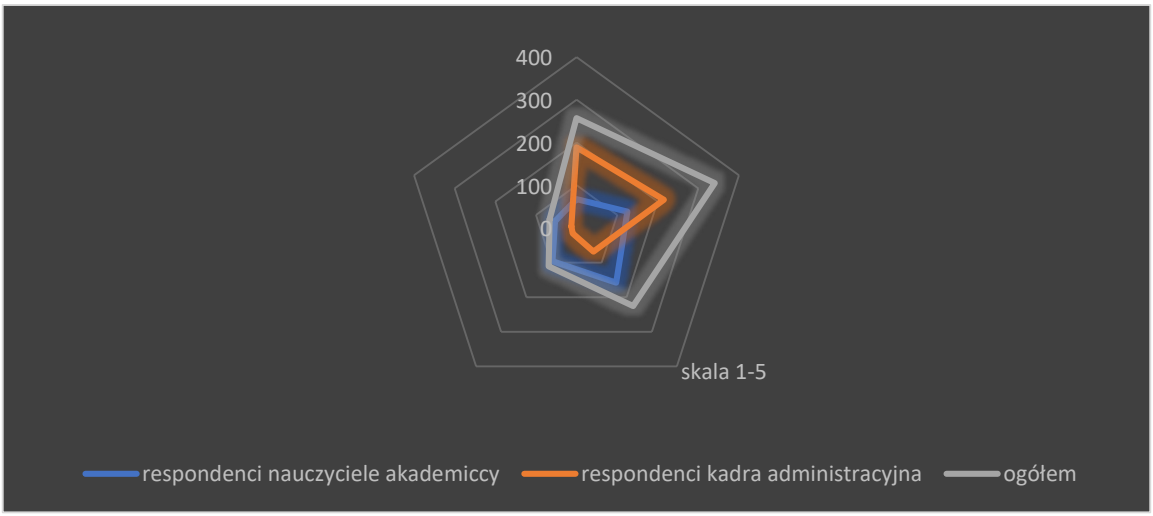
Tabela 2.13. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy kadra administracyjna na temat najczęściej wykorzystywanego kanału do przekazywania informacji, jakim jest Aplikacja MsTeams

Odpowiedzi badanych osób • **Zastosowany rodzaj kanału obiegu informacji (Aplikacja MsTeams)**									
Osoby poddane badaniu	**Respondenci nauczyciele akademiccy**			**Respondenci kadra administracyjna**			**OGÓŁEM**		
Ocena od 1-5	***liczba wskazań***	***udział procentowy***	***ocena średnia***	***liczba wskazań***	***udział procentowy***	***ocena średnia***	***liczba wskazań***	***udział procentowy***	***ocena średnia***
1	68	13,6%	0,14	189	37,8%	0,38	257	25,7%	0,26
2	125	25%	0,5	215	43%	0,86	340	34%	0,68
3	158	31,6%	0,95	68	13,6%	0,41	226	22,6%	0,68
4	96	19,2%	0,77	15	3%	0,12	111	11,1%	0,44
5	53	10,6%	0,53	13	2,6%	0,13	66	6,6%	0,33
	500	**100%**	**2,89**	**500**	**100%**	**1,9**	**1000**	**100%**	**2,39**

Źródło: opracowanie własne na podstawie badań własnych

W badaniu wzięło udział 500 osób zatrudnionych na stanowisku, nauczycieli akademickich oraz 500 osób zatrudnionych na stanowisku kadry administracyjnej. Wszystkie wyżej wskazane osoby poprawnie udzieliły odpowiedzi w ilości 100%. Nie doszło do sytuacji, w której odpowiedzi zostały błędnie wskazane. W przypadku nauczycieli akademickich najwyższą (najczęstszą) odpowiedź odnośnie kanału przekazywania informacji, jaką jest *Aplikacja MsTeams* udzieliło 53 respondentów to jest 10,6%. Najniższą odpowiedź (najrzadziej) korzysta z tej drogi przekazu informacji 68 osoby to jest 13,6%. Badania pokazują, że w dalszym ciągu dużo nauczycieli akademickich nie korzysta z tej formy przekazywania informacji. Widoczny jest tu bilans między ilością osób korzystających z aplikacji oraz z ilością osób, które z niej bardzo rzadko korzystają. Kadra administracyjna zadeklarowała najwyższą (najczęstszą) drogę przesyłu informacji w ilości 13 respondentów to jest 2,6%. Liczba wskazań dla najniższej oceny to 189 respondentów, którzy zadeklarowali tą odpowiedź. Jest to 37,8%.

Wykres 2.25. Odpowiedzi respondentów pracowników grupy nauczyciele akademiccy i grupy kadra administracyjna na temat najczęściej wykorzystywanego kanału do przekazywania informacji, jakim jest aplikacja MsTeams



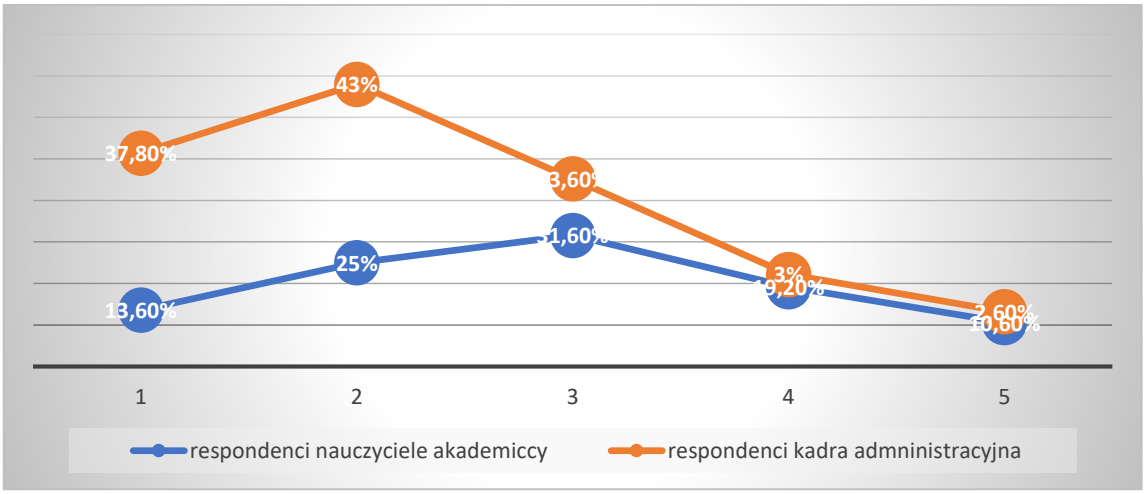
Źródło: opracowanie własne na podstawie badań własnych

Ogólna ocena średnia dla grupy nauczycieli akademickich wynosi 2,89%, zaś dla kadry administracyjnej wynosi 1,9%. Istnieje zależność między zmiennymi a świadczy o tym współczynnik korelacji liniowej Pearsona na poziomie 0,16 i współczynnik determinacji liniowej, wskazujący procent wyjaśnionej liniowo zmienności równy 2,56%.

$$r_{xy} = \frac{\frac{1}{n}\sum_{i=1}^{n}(x_i-\bar{x})(y_i-\bar{y})}{S_x S_y}=0{,}16$$

$$\mathrm{WD}=r_{xy}^{2} * 100\% = 2{,}56\%$$

Wykres 2.26. Zależność między respondentami grupy nauczyciele akademiccy i grupy kadra administracyjna pod względem najczęściej wykorzystywanego kanału do przekazywania informacji, jakim jest aplikacja MsTeams



Źródło: opracowanie własne na podstawie badań własnych

Reasumując, rozkład badanych zmiennych wskazuje, że nauczyciele akademiccy częściej korzystają z tej formy przekazu informacji niż kadra administracyjna. Tak niskie deklaracje mogą być spowodowane faktem dosyć krótkiego korzystania z wspomnianej aplikacji. Konieczność, która wynikała z potrzeby korzystania wynikała z sytuacji panującej w kraju od roku 2020 a związanej z Covid-19. W tabeli 2.14 zaprezentowano rozkład odpowiedzi na temat wykorzystanego w uczelni wyższej kanału obiegu informacji, jakim jest aplikacja MsTeams. Zostały porównane 2 grupy respondentów nauczyciele akademiccy i studenci (różne roczniki).

Tabela 2.14. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy studentów (różne roczniki) na temat najczęściej wykorzystywanego kanału do przekazywania informacji, jakim jest Aplikacja MsTeams

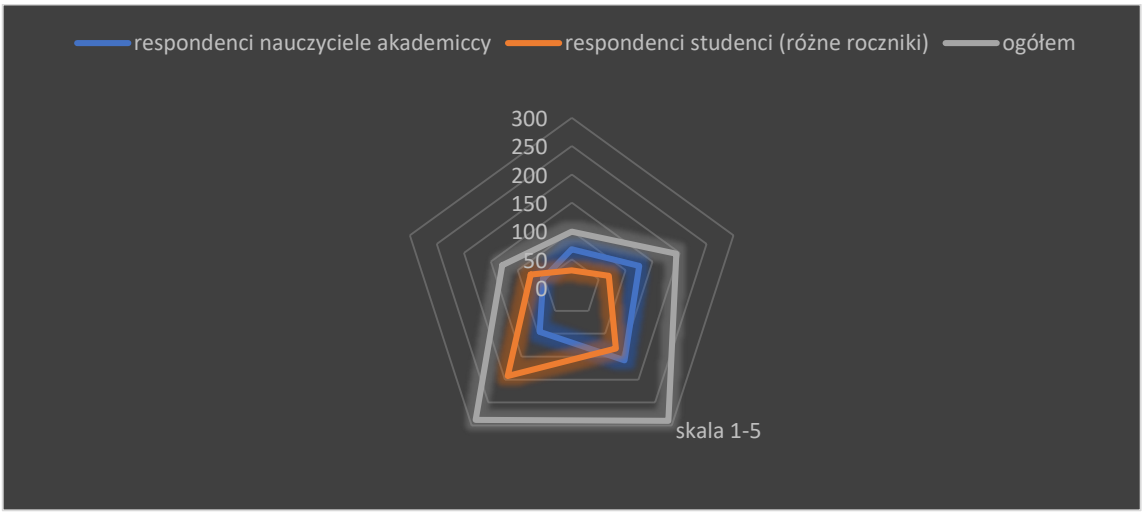
Odpowiedzi badanych osób • **Zastosowany rodzaj kanału obiegu informacji (Aplikacja Ms Teams)**									
Osoby poddane badaniu	**Respondenci nauczyciele akademiccy**			**Respondenci studenci (różne kierunki)**			**OGÓŁEM**		
Ocena od 1-5	***liczba wskazań***	***udział procentowy***	***ocena średnia***	***liczba wskazań***	***udział procentowy***	***ocena średnia***	***liczba wskazań***	***udział procentowy***	***ocena średnia***
1	68	13,6%	0,14	31	6,2%	0,06	99	9,9%	0,1
2	125	25%	0,5	69	13,8%	0,28	194	19,4%	0,39
3	158	31,6%	0,95	132	26,4%	0,79	290	29%	0,87
4	96	19,2%	0,77	192	38,4%	1,54	288	28,8%	1,152
5	53	10,6%	0,53	76	15,2%	0,76	129	12,9%	0,64
	500	**100%**	**2,89**	**500**	**100%**	**3,43**	**1000**	**100%**	**3,15**

Źródło: opracowanie własne na podstawie badań własnych

W badaniu wzięło udział 500 osób zatrudnionych na stanowisku, nauczycieli akademickich oraz 500 osób studiujących na uczelni wyższej. Wszystkie wyżej wskazane

osoby poprawnie udzieliły odpowiedzi w ilości 100%. Nie doszło do sytuacji, w której odpowiedzi zostały błędnie wskazane. W przypadku nauczycieli akademickich najwyższą (najczęstszą) odpowiedź odnośnie kanału przekazywania informacji, jaką jest *Aplikacja MsTeams* udzieliło 53 respondentów to jest 10,6%. Najniższą odpowiedź (najrzadziej) korzysta z tej drogi przekazu informacji 68 osoby to jest 13,6%. Badania pokazują, że w dalszym ciągu dużo nauczycieli akademickich nie korzysta z tej formy przekazywania informacji. Widoczny jest tu bilans między ilością osób korzystających z aplikacji oraz z ilością osób, które z niej bardzo rzadko korzystają. Studenci zadeklarowali najwyższą (najczęstszą) drogę przesyłu informacji w ilości 176 to jest 0,76%. Liczba wskazań dla najniższej oceny to 31 respondentów, którzy zadeklarowali tą odpowiedź, jest to 6,2%

Wykres 2.27. Odpowiedzi respondentów pracowników grupy nauczyciele akademiccy i grupy studentów (różnych roczników) na temat najczęściej wykorzystywanego kanału do przekazywania informacji, jakim jest aplikacja MsTeams



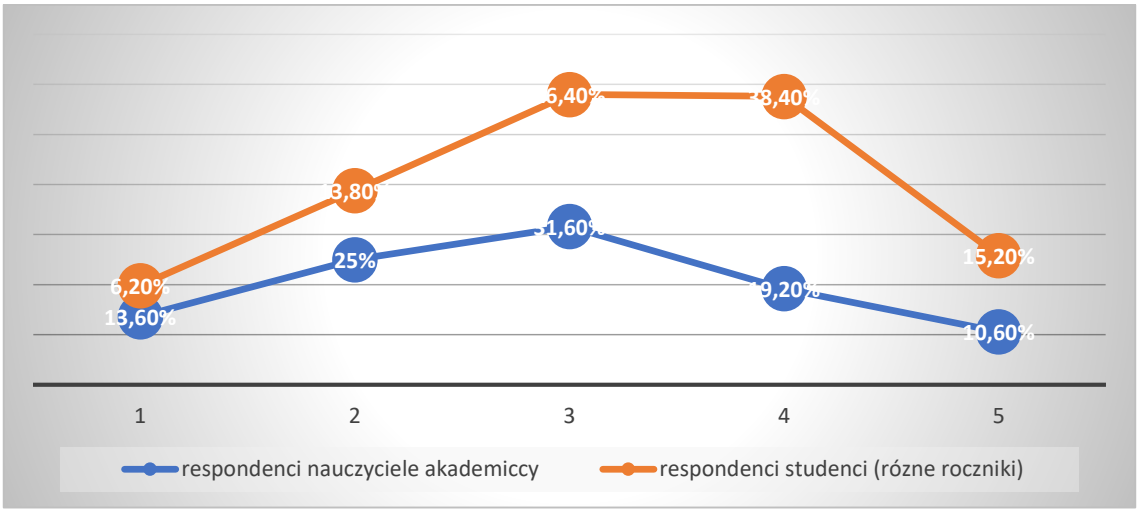
Źródło: opracowanie własne na podstawie badań własnych

Ogólna ocena średnia dla grupy nauczycieli akademickich wynosi 2,89%, zaś dla studentów wynosi 3,43%. Istnieje zależność między zmiennymi a świadczy o tym współczynnik korelacji liniowej Pearsona na poziomie 0,38 i współczynnik determinacji liniowej, wskazujący procent wyjaśnionej liniowo zmienności i jest równy 14,44%.

$$r_{xy} = \frac{\frac{1}{n}\sum_{i=1}^{n}(x_i-\bar{x})(y_i-\bar{y})}{S_x S_y}=0{,}38$$

$$\mathrm{WD}=r_{xy}^{2} * 100\% = 14{,}44\%$$

Wykres 2.28. Zależność między respondentami grupy nauczyciele akademiccy i grupy studenci (różne roczniki) pod względem najczęściej wykorzystywanego kanału do przekazywania informacji, jakim jest aplikacja MsTeams



Źródło: opracowanie własne na podstawie badań własnych

Reasumując, rozkład badanych zmiennych wskazuje, że zarówno nauczyciele akademiccy jak i studenci korzystają w małym stopniu z MsTeams. Należy przypuszczać, że powodem może być fakt korzystania z tej aplikacji tylko w związku z koniecznością przeprowadzenia lub uczestnictwa w zajęciach. W tabeli 2.15. zaprezentowano rozkład odpowiedzi na temat wykorzystanego w uczelni wyższej kanału obiegu informacji, jakim jest aplikacja MsTeams. Zostały porównane 2 grupy respondentów kadra administracyjna i studenci (różne roczniki).

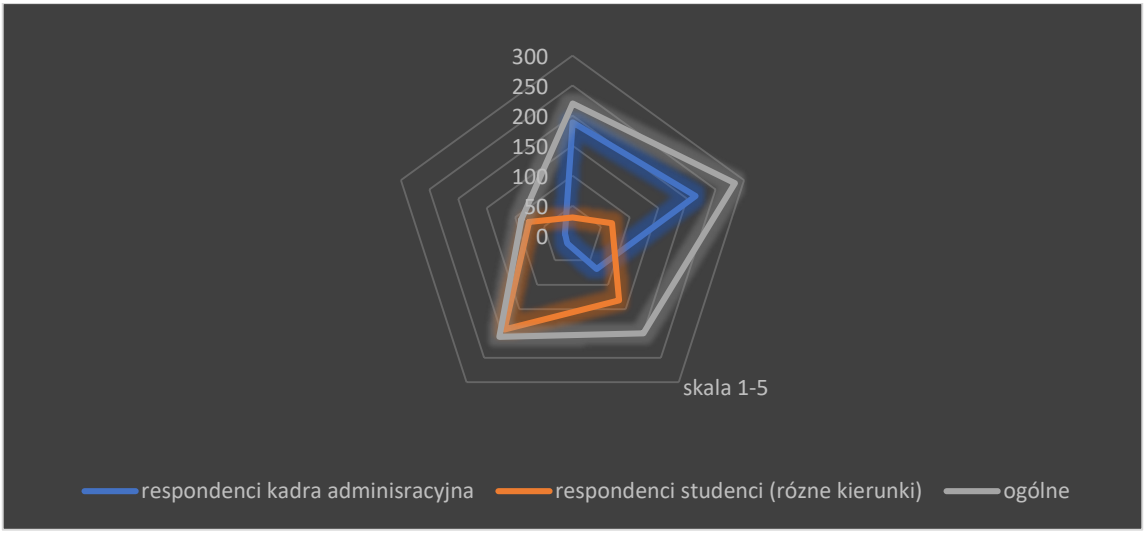
Tabela 2.15. Odpowiedzi respondentów grupy kadra administracyjna i grupy studentów (różne roczniki) na temat najczęściej wykorzystywanego kanału do przekazywania informacji, jakim jest Aplikacja MsTeams

Odpowiedzi badanych osób • **Zastosowany rodzaj kanału obiegu informacji (Aplikacja MsTeams)**									
Osoby poddane badaniu	**Respondenci kadra administracyjna**			**Respondenci studenci (różne kierunki)**			**OGÓŁEM**		
Ocena od 1-5	***liczba wskazań***	***udział procentowy***	***ocena średnia***	***liczba wskazań***	***udział procentowy***	***ocena średnia***	***liczba wskazań***	***udział procentowy***	***ocena średnia***
1	189	37,8%	0,38	31	6,2%	0,06	220	22%	0,22
2	215	43%	0,86	69	13,8%	0,28	284	28,8%	0,58
3	68	13,6%	0,41	132	26,4%	0,79	200	20%	0,6
4	15	3%	0,12	192	38,4%	1,54	207	20,7%	0,83
5	13	2,6%	0,13	76	15,2%	0,76	89	8,9%	0,44
	500	**100%**	**1,9**	**500**	**100%**	**3,43**	**1000**	**100%**	**2,67**

Źródło: opracowanie własne na podstawie badań własnych

W badaniu wzięło udział 500 osób zatrudnionych na stanowisku, kadry administracyjnej oraz 500 osób studiujących w uczelni wyższej. Wszystkie wyżej wskazane osoby poprawnie udzieliły odpowiedzi w ilości 100%. Nie doszło do sytuacji, w której odpowiedzi zostały błędnie wskazane. W przypadku kadry administracyjnej najwyższą (najczęstszą) odpowiedź odnośnie kanału przekazywania informacji, jaką jest *aplikacja MsTeams* udzieliło 13 respondentów to jest 2,6%. Najniższą odpowiedź (najrzadziej) korzysta z tej drogi przekazu informacji 189 osoby to jest 37,8%. Studenci zadeklarowali najwyższą (najczęstszą) drogę przesyłu informacji w ilości 76 respondentów to jest 15,2%. Najniższa ocena w przypadku studentów to 31 wskazań, czyli 6,2%.

Wykres 2.29. Odpowiedzi respondentów pracowników grupy kadra administracyjna i grupy studentów (różnych roczników) na temat najczęściej wykorzystywanego kanału do przekazywania informacji, jakim jest aplikacja MsTeams



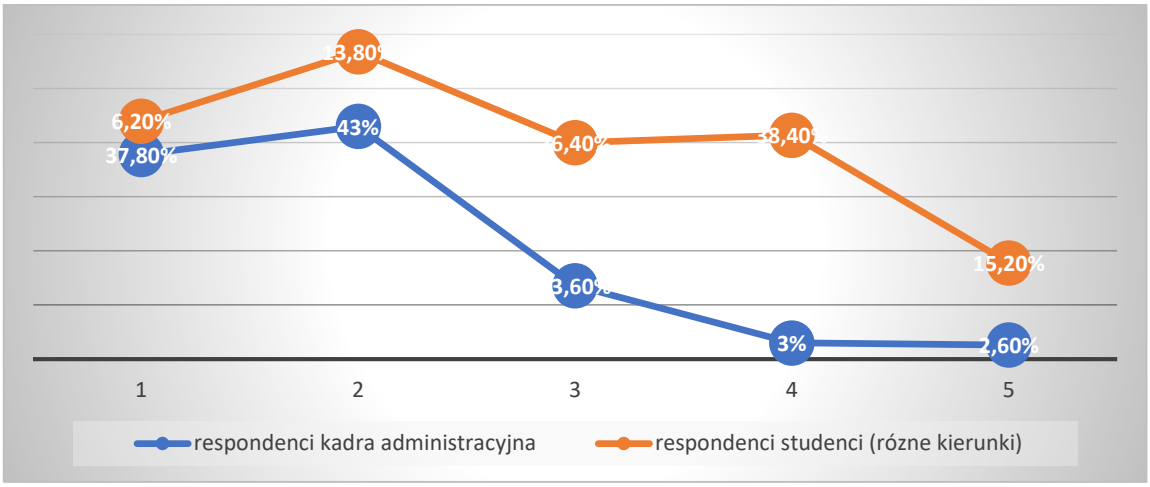
Źródło: opracowanie własne na podstawie badań własnych

Ogólna ocena średnia dla grupy kadry administracyjnej wynosi 1,9%, zaś dla studentów wynosi 3,43%. Wzrost wartości jednej zmiennej wiąże się ze spadkiem wartości zmiennej drugiej a świadczy o tym współczynnik korelacji liniowej Pearsona na poziomie -0,68 i współczynnik determinacji liniowej, wskazujący procent wyjaśnionej liniowo zmienności i jest równy 46,24%.

$$r_{xy} = \frac{\frac{1}{n}\sum_{i=1}^{n}(x_i-\bar{x})(y_i-\bar{y})}{S_x S_y} = -0{,}68$$

$$\mathrm{WD} = r_{xy}^{2} * 100\% = 46{,}24\%$$

Wykres 2.30. Zależność między respondentami grupy kadra administracyjna i grupy studenci (różne roczniki) pod względem najczęściej wykorzystywanego kanału do przekazywania informacji, jakim jest aplikacja MsTeams



Źródło: opracowanie własne na podstawie badań własnych

Reasumując, rozkład badanych zmiennych wskazuje, że kadra administracyjna rzadziej korzysta z aplikacji MsTeams niż studenci. Zaistniała sytuacja wskazuje, że kadra administracyjna najprawdopodobniej korzysta z innych form przekazu informacji. W tabeli 2.16. znajduje się podział pod względem najczęściej wykorzystywanego kanału przekazywania informacji w uczelni wyższej.

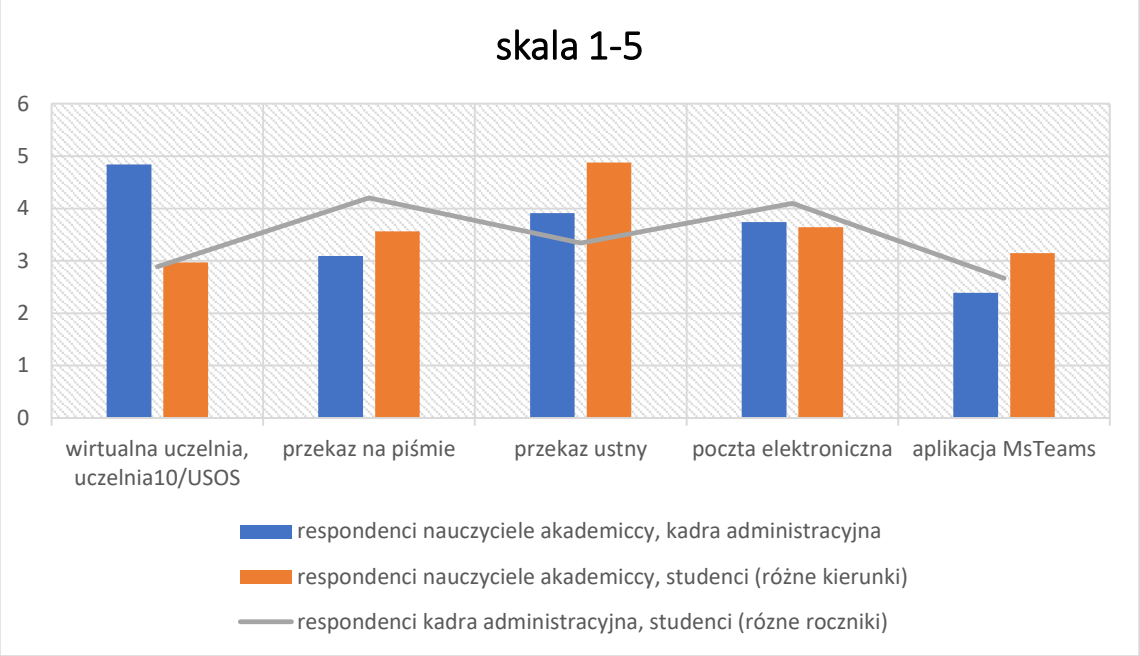
Tabela 2.16. Podział pod względem najczęściej wykorzystywanego kanału przekazywania informacji w uczelni wyższej

Odpowiedzi respondentów – najczęstszy kanał przekazywania informacji				
Osoby poddane badaniu	**Respondenci, nauczyciele akademiccy, kadra administracyjna**	**Respondenci, nauczyciele akademiccy, studenci (różne kierunki)**	**Respondenci, kadra administracyjna, studenci (różne roczniki)**	**Ogólna ocena**
	Skala 1-5	***Skala 1-5***	***Skala 1-5***	***Skala 1-5***
Wirtualna uczelnia, uczelnia 10/USOS	**4,84**	**2,97**	**2,89**	**3,57**
Przekaz na piśmie	**3,09**	**3,56**	**4,20**	**3,62**
Przekaz ustny	**3,91**	**4,88**	**3,34**	**4,04**
Poczta elektroniczna	**3,74**	**3,64**	**4,10**	**3,83**
Aplikacja MsTeams	**2,39**	**3,15**	**2,67**	**2,74**

Źródło: opracowanie własne na podstawie badań własnych

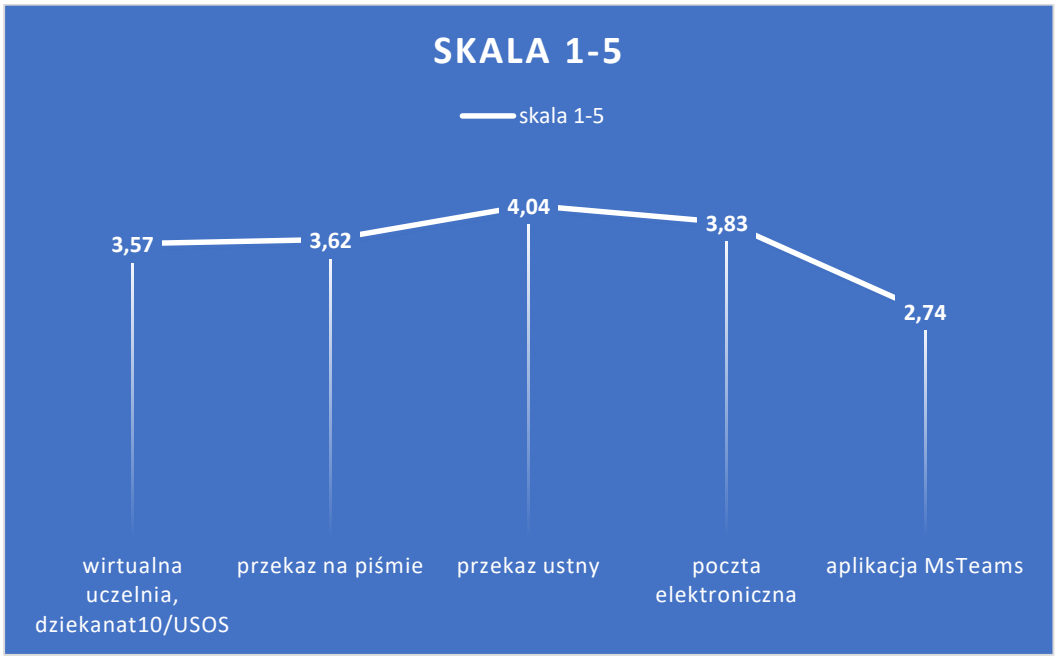
Poniżej na wykresach 2.31 i 2.32 przedstawione zostały dane dotyczące podziału pod względem najczęściej wykorzystywanego kanału przekazywania informacji w uczelni wyższej.

Wykres 2.31. Podziała pod względem najczęściej wykorzystywanego kanału przekazywania informacji w uczelni wyższej



Źródło: opracowanie własne na podstawie badań własnych

Wykres 2.32. Ranking podziału pod względem najczęściej wykorzystywanego kanału przekazywania informacji w uczelni wyższej



Źródło: opracowanie własne na podstawie badań własnych

Badania empiryczne dowiodły, że w publicznej uczelni wyższej najczęstszym kanałem wykorzystywanym do obiegu informacji wśród respondentów jest przekaz ustny.

Respondenci ocenili swoją częstotliwość korzystania z tej formy przekazywania informacji po uśrednieniu na poziomie 4,04 z 5. Następnie respondenci wskazali na pocztę elektroniczną, która w średniej ocenie uzyskała wynik 3,83 z 5. Z badań wynika, że w dalszej kolejności wśród zbiorowości uczelnianej wykorzystuje się informacje na piśmie, gdzie średnia ocena to 3,62 z 5. Wśród badanych kanałów obiegu informacji przed ostatnią pozycję zajęła wirtualna uczelnia, dziekanat10/USOS, gdzie przypisano jej średnią ocenę 3,57 z 5. Najmniej respondentów wskazało na wykorzystanie do obiegu informacji w uczelni wyższej aplikacji MsTeams, 2,74. Należy stwierdzić, że przekaz ustny jest nadal bardzo popularną i wiążącą formą przekazywani informacji. Jednakże pozostałe alternatywne odpowiedzi również są oceniane bardzo wysoko.

Dzięki wdrożeniom odpowiednich środków ochrony informacji, systemu zarządzania bezpieczeństwem informacji rektor uczelni wyższej ma możliwość:

- zapewnienia odpowiednich warunków mających na celu realizację przyjętej misji uczelni wyższej;
- zapewnienie ciągłości i sprawności organizacyjnej;
- zapewnienie dobrej marki organizacji na poziomie innych publicznych uczelni wyższych;
- zapewnienie gwarantujące niezawodność procesów w aspekcie terminowości, dostępności informacji, integralności informacji oraz jej poufności;
- zapewnienie realizacji przepisów prawnych w ochronie m.in. tajemnicy państwowej lub danych osobowych[1].

Na rektorze uczelni wyższej spoczywa obowiązek kierowania pracą związaną z przetwarzaniem, zasilaniem, udostępnianiem oraz archiwizowaniem informacji znajdujących się w bazie danych. Jest również odpowiedzialny za szkolenia pracowników w zakresie metod ochrony danych, jak i szkolenia związane z pojawiającymi się sytuacjami losowymi zdarzeń będących zagrożeniem dla organizacji. Ponadto rektor, jako główny administrator baz danych sprawuje nadzór nad tzw. integralnością, jakością w szerszym znaczeniu, czyli kompletnością, aktualnością. Ważną kwestią, o jakiej należy wspomnieć jest odpowiednie działanie dotyczące takiego procesu jak kopiowanie baz danych, odzyskiwanie, sterowanie dostępem do danych[2].

[1] K. Liderman, *Bezpieczeństwo…dz. cyt.*, s. 158.
[2] W. Flakiewicz, *Systemy informacyjne w zarządzaniu…dz. cyt.*, s. 120.

W ramach procesu informacyjnego dokonuje się zaspokojenia potrzeb informacyjnych i jako element integrujący i sterujący podstawowymi jak i pomocniczymi działaniami zmierzającymi poprzez realizacje wytyczonych zadań do osiągnięcia celów publicznej uczelni wyższej i ma nieodzowny wpływ na skuteczność procesu decyzyjnego[1]. Po dokonanej diagnostyce systemu informacyjnego w uczelni wyższej, zostało określone otoczenie wewnętrzne badanej organizacji, Został zbadany kanał przekazywania i odbioru informacji przez użytkowników systemu informacyjnego działającego w publicznej uczelni wyższej.

Wnioski

Przeprowadzone działania dały możliwość rozwiązania problemu badawczego odpowiadającego na postawione pytanie: ***Jakie uwarunkowania wpływają na bezpieczeństwo systemu informacyjnego w uczelni wyższej?*** a zarazem weryfikację przyjętej hipotezy, która zakładała, iż *bezpieczeństwo systemu informacyjnego przekłada się na bezpieczeństwo interesariuszy uczelni wyższej i świadczy o wysokim standardzie zarządzania jednostką organizacyjną.* Dzięki posiadanemu doświadczeniu i bazując na badaniach empirycznych i teoretycznych zostały doprecyzowane *wnioski.*

Szczególnie ważnym jest fakt, że „kierownik" powinien zwiększyć kontrolę kanału obiegu informacji i aby zapewnić pełne bezpieczeństwo wszystkich użytkowników, systemu informacyjnego powinien to właśnie on na powyższych działaniach się skoncentrować. Wymagane jest wprowadzenie na uczelni wyższej zabezpieczeń systemowych mających na celu uniemożliwienie logowania do kont prywatnych, e-mailowych oraz przesyłanie danych.

W uczelni wyższej należy wprowadzić zakaz wynoszenia na zewnątrz laptopów zawierających dane osobowe, których utrata mogłaby działać na niekorzyść pracownika, jednostki a nawet całej organizacji. Brane są tu pod uwagę dane wrażliwe, jawne i niejawne. Nie powinno się również zabierać dysków ani innych nośników, które nie posiadają wprowadzonego hasła. W związku z powyższym pracownicy powinni mieć stanowiska pracy przystosowane do potrzeb indywidualnych z dostępem do systemu informacyjnego z pełnym zabezpieczeniem systemu a przydzielone zadania nie powinny zmuszać pracownika do wykonywania zaległych czynności poza miejscem pracy.

[1] G. Michalczewski, *Czynniki kształtujące potrzeby informacyjne, [w:] Procesy informacyjne w obronności i bezpieczeństwie. Teoria i praktyka*, red. M. Wrzosek, Wydawnictwo Akademii Sztuki Wojennej, Warszawa 2017, s. 47.

Ważnym aspektem jest ciągłe wdrażanie procedur i zabezpieczeń informacji. Droga elektroniczna w szczególności e-maile pracownicze powinny być szczególnie zabezpieczone, aby nie dochodziło do przepuszczania tzw. spamu z różnego rodzaju reklamami, linkami mogącymi zawierać wirusy. Kadra uczelniana w szczególności powinna systematycznie korzystać z dodatkowych szkoleń dotyczących podwyższenia świadomości jak i podniesienia kompetencji. Powyżej wspomniane dodatkowe działania powinny być dostępne dla wszystkich użytkowników systemów informacyjnych z włączeniem oprócz pracowników zatrudnionych na etatach i umowach zlecenie także studentów i osób zewnętrznych.

W celu zwiększenia bezpieczeństwa systemu informacyjnego należy zakupić specjalne oprogramowania, zakupić nowy sprzęt i zamortyzować ten, który jest już leciwy. Taki sprzęt szybko ulega wszelkim awariom a dane na nim zapisane mogą ulec utraceniu. Przestaje on też spełniać swoje funkcje poprzez *zawodność*, co może zdezorganizować pracę. W ramach efektywnego zarządzania bezpieczeństwem powinny być wyznaczone dodatkowe osoby, mogące na bieżąco analizować poziom bezpieczeństwa systemu informacyjnego w uczelni wyższej.

Potrzeba dodatkowych osób wynika z konieczności obsługi tak dużej społeczności akademickiej, odbierania sygnałów od użytkowników o zaistniałych problemach, szybkiego reagowania na zaistniałe niepokojące incydenty i szybkie działania wdrażające, polegające na nowych zabezpieczeniach chroniących przed cyberprzestępcami.

3. ZAGROŻENIA BEZPIECZEŃSTWA SYSTEMU INFORMACYJNEGO

Zastosowanie systemów informatycznych wiąże się z pewnym ryzykiem zagrożenia. Kwestią nieodzowną i bardzo istotną jest fakt, w którym użytkownicy tych wdrożonych systemów powinni zrozumieć i przewidzieć sytuację, w której może pojawić się zagrożenie, móc sprawnie zareagować jak już dojdzie do takiego zdarzenia. W związku z powyższym skupienie się na problemach dotyczących bezpieczeństwa systemu informacyjnego wydaje się być zasadne, znaczące z punktu widzenia ochrony zasobów publicznej uczelni wyższej. Badania, które zostały przeprowadzone miały na celu otrzymanie odpowiedzi na szczegółowy problem badawczy zawierający się w pytaniu:, *Jakie występują zagrożenia bezpieczeństwa systemu informacyjnego?* A przy okazji zweryfikowanie przyjętej hipotezy *mającej stanowić przypuszczenie, iż zagrożenia w bezpieczeństwie systemu informacyjnego w publicznej uczelni wyższej występują, ponieważ dotychczasowe zabezpieczenia przekazywania informacji i procedury bezpieczeństwa informacyjnego nie były przez użytkowników w należyty sposób przestrzegane.*

Autorka założyła, że w związku z tak dużą ilością pracowników użytkujących system informacyjny w uczelni wyższej, zmniejsza się jego poziom bezpieczeństwa poprzez częściowe wykorzystanie wszystkich zabezpieczeń oraz procedur, które w tym przypadku nie mają istotnego wpływu. Niektórzy użytkownicy nie mieli świadomości konsekwencji łamania zasad korzystania z tego systemu. Nie poczuwali się do spadającej na nich odpowiedzialności za poprawne korzystanie.

Przypuszczalnym jest fakt, że typowe zagrożenia systemu bezpieczeństwa obiegu informacji polegają na takich działaniach jak:

- przestępstwa wykorzystujące komputer, laptop, tablet, telefon oraz urządzenia i nośniki, na których znajdują się dane;
- utrata informacji związanych z włamaniem na urządzenia poprzez przesyłanie np. zawirusowanych wiadomości, złośliwe kody, linki;
- cyberterroryzm,
- szpiegostwo,
- sabotaż,
- wandalizm.

Rozpoznanie, doskonalenie, utrzymanie bezpieczeństwa informacyjnego staję się podstawą do zapewnienia przewagi nad konkurencją innych mniej przychylnych organizacji.

Możliwość zlokalizowania źródeł zagrożenia pozwala na wyłonienie zagrożenia systemu bezpieczeństwa informacyjnego powstającego wewnątrz organizacji. Do najczęstszych zagrożeń należy zaliczyć m.in.:

- uszkodzenie danych w przypadku złego użytkowania;
- utrata danych w przypadku zagubienia czy kradzieży;
- brak możliwości obsługi danych w związku z pojawiającym się błędem spowodowanych działaniami nieumyślnymi w sytuacjach losowych;
- utrata danych poprzez celowe uszkodzenie nieuczciwych użytkowników.

Można wyodrębnić także zagrożenia fizyczne a szkoda w nich spowodowana jest awarią, wypadkiem, bądź innym niedającym się przewidzieć zdarzeniem mającym szeroki wpływ na system informacyjny. Takie zdarzenia można podzielić na:

- zagrożenia informacyjne tradycyjne, działalność dywersyjna, sabotażowa, szpiegostwo, ofensywa dezinformacyjna prowadzona przez obce osoby, podmioty, organizacje a nawet państwa;
- zagrożenia losowe, wypadki, katastrofy, klęski żywiołowe, powodzie, pożary (zagrożenia związane ściśle z organizacją);
- zagrożenia technologiczne, zagrożenia mające ścisły związek z gromadzeniem, przetwarzaniem, przekazywaniem informacji, danych w sieciach teleinformatycznych;
- zagrożenia mające swoje odniesienie do obywatelskich praw m.in. sprzedaż lub przekazywanie informacji podmiotom do tego nieuprawnionym.

Reasumując wszystkie wątki założono, że elementami bezpośrednio mającymi decydować o bezpieczeństwie obiegu informacji były po pierwsze brak wiedzy, poczucia odpowiedzialności pracowników uczestniczących w procesie obiegu informacji. Po drugie wszystkie inne elementy napływające z zewnątrz mające podłoże przestępcze. W dobie tak szybkiego rozwoju bezpieczeństwo obiegu informacji mogą zagłuszyć takie elementy jak ciekawość, korupcja.

W związku z potrzebą udzielenia odpowiedzi na problem badawczy oraz weryfikację hipotezy w rozdziale 3 zostały zastosowane metody badawcze takie jak:

- *analiza* – została zastosowana do weryfikacji literatury specjalistycznej przedmiotu, aktów normatywnych jak i dokumentacji uczelnianej;

- *synteza* – została wykorzystana do poznania istoty zjawiska jak również scalenia pozyskanych wyników analizy w jedną syntetyczną całość;
- *abstrahowanie* – metoda ta została wykorzystana podczas wyodrębniania elementów przedmiotu badań, uznanych za drugorzędne i nieistotne[1];
- *uogólnienie* – zastosowano przy określeniu poziomu bezpieczeństwa badanego systemu informacyjnego, uwzględnione zostało środowisko wewnętrzne uczelni wyższej a polegało na łączeniu podobnych faktów;
- *porównanie* – miało swoje zastosowanie przy identyfikacji cech wspólnych, różnic, podobieństw i dotyczyło poszczególnych zagadnień badawczych. Szczególnie przydatne było w zakresie obiegu informacji oraz bezpieczeństwa tego procesu w organizacji publicznej, uczelni wyższej;
- *wnioskowanie* – wykorzystane we wszystkich rozdziałach znajdujących się w pracy doktorskiej, w części poświęconej wnioskom i w zakończeniu dysertacji;
- *dedukcja* – wykorzystana została do uogólnienia, wskazania wszystkich czynników, które mogą wpłynąć na bezpieczeństwo systemu informacyjnego w uczelni wyższej;
- *redukcja* – miała zastosowanie i przełożyła się na wskazanie i opisanie rezultatów stosowania systemu obiegu informacji w uczelni wyższej, jako organizacji publicznej[2];
- *obserwacja* – została wykorzystana do przemyśleń nad sytuacją problemową a która wychodzi naprzeciw podjętym badaniom i sformułowaniu celu ich prowadzenia i na końcu, wyłonienie trafnej analizy oraz interpretacji;
- *metoda sondażu diagnostycznego* [3] – zastosowana została *technika ankiety,* dzięki niej była możliwość pozyskania opinii respondentów ich postrzeganie dot. zjawiska badanego. Nastąpiło wykorzystanie *techniki wywiadu eksperckiego*, którego niezmiennym celem było poznanie opinii eksperta w zakresie systemu informacyjnego działającego w uczelni wyższej.

[1] E. Wiśniewski, *Metodyka wojskowych…dz. cyt.*, s. 74.
[2] W. Pytkowski, *Organizacja badań…dz. cyt.*, s. 117-124.
[3] J. Apanowicz, *Metodologia nauk…dz. cyt.*, s. 25-51.

3.1. Wyzwania i zagrożenia bezpieczeństwa systemu informacyjnego

Opisując system informacyjny należy odnieść się do pojęcia, jakim jest zagrożenie a mianowicie jest to stan lub sytuacja, w której personalnie ktoś czuje się zagrożony bądź komuś zagrażają, taką sytuację może stworzyć osoba. W odniesieniu do słowa zagrozić to sytuacja, która ujawnia się zmuszeniem konkretnej osoby do określonego czynu[1].

Zagrożenie to nic innego jak sytuacja, w której następuje pojawienie się prawdopodobieństwa powstania stanu niebezpiecznego dla otoczenia[2]. W publikacjach naukowych zagrożenie jest postrzegane pod różnymi aspektami. Dwie definicje zagrożenia zostały zaproponowane przez K. Liedela. Pierwsza z nich jest w ujęciu subiektywnym i wskazuje na pewien stan psychiki i świadomości wywołany postrzeganiem zjawisk, jako niekorzystnych czy niebezpiecznych. W drugim ujęciu realnym zagrożeniem jest definiowane, jako rzeczywiste niebezpieczeństwo powodujące stan obaw i niepewności[3].

Najczęstszą strategią w walce o zapewnienie bezpieczeństwa jednostki jest unikanie zagrożeń. Jednakże nie zawsze jest wystarczające i skuteczne. Obydwa te otoczenia zarówno bliższe, jaki dalsze kreują poziom bezpieczeństwa. B. Hołyst pisze, że zagrożenie nie jest jednoznaczne, ponieważ jest to sytuacja uświadomiona przez dotknięty danym zdarzeniem przedmiot. W odniesieniu badacza zagrożenie danego podmiotu zachodzi w czasie, kiedy „w człowieku rodzi się obawa o utratę wysoko cenionych wartości z własnym życiem na pierwszym miejscu” [4]. Zdaniem W. Fehlera zagrożenie jest postrzegane w intuicyjnym odbiorze, jako przeciwieństwo bezpieczeństwa. Oznacza taką sytuację, w której istotne dla danego podmiotu wartości stają się trudno dostępne[5]. Zagrożenia bezpieczeństwa pod względem ich zasięgu R. Kuriata podzielił na trzy grupy:

- zagrożenia lokalne, powstają na terytorium gminy i powiatu;
- zagrożenia regionalne, powstają na terenie województwa;
- zagrożenia narodowe, prowadzić mogą do zerwania więzi społecznych i problemów politycznych czy gospodarczych[6].

---

[1] www.sjp.pwn.pl [dostęp: 1.12.2022].
[2] J. Pawłowski, *Słownik terminów z zakresu bezpieczeństwa narodowego,* AON, Warszawa 2002, s. 172–173.
[3] K. Liedel, *Bezpieczeństwo informacyjne w dobie terrorystycznych…dz. cyt.,* s. 8.
[4] B. Hołyst, Wiktymologia, PWN, Warszawa 1997, s. 64-65.
[5] W. Fehler, *Zagrożenie – kluczowa kategoria teorii bezpieczeństwa, [w:] Współczesne postrzeganie bezpieczeństwa*, red. K. Jałoszyński, B. Wiśniewski, T. Wojtuszek, WSA, Bielsko--Biała 2007, s. 34.
[6] M. Cieślarczyk, R. Kuriata, *Kryzys i sposoby radzenia sobie z nim,* Wydawnictwo Naukowe Wyższej Szkoły Kupieckiej, Łódź 2005, s. 71.

W ocenie Lidermana najczęstszymi kryteriami, warunkującymi bezpieczeństwo informacyjne są: tajność, integralność, dostępność a zagrożenia skwalifikował następująco:

- siły wyższe;
- nieuprawnione i przestępcze działanie ludzi, podsłuchy, nieuprawnione działania personelu, osób postronnych;
- wkradające się błędy ludzi uczestniczących w procesach przetwarzania informacji;
- błędy w organizacji przetwarzania informacji;
- błędy w oprogramowaniu i awarie sprzętu;
- awarie infrastruktury usługowej[1].

Według opinii R. J. Suttona, poufne informacje, często pocztą elektroniczną są przesyłane bez zastanowienia.

Informacje takie, jak oceny, dane osobowe i finansowe, oferty prawnie zastrzeżone szczegóły techniczne, dane personalne oraz wiele innych, których ujawnienie może spowodować szkody, są często przesyłane, jako niechronione. Mimo tego, że dany pracownik posiada możliwość kodowania plików czasem z beztroski czy nie świadomości lub zaoszczędzenia kilku minut przesyła w formie bezpośredniego podglądu. Badacz ten wiąże zagrożenia bezpieczeństwa informacyjnego z podsłuchiwaniem, modyfikowaniem, powtarzaniem, penetrowaniem, zakłócaniem[2].

P. Bączko w swoim katalogu zagrożeń bezpieczeństwa informacyjnego wskazał:

- z*agrożenia losowe,* klęski, katastrofy, wypadki, które w dużym stopniu wpływają na stan bezpieczeństwa informacyjnego;
- *zagrożenia informacyjne tradycyjne*, szpiegostwo, sabotaż;
- *zagrożenia technologiczne,* zagrożenia w szczególności powiązane z gromadzeniem, przetwarzaniem, przekazywaniem informacji w sieciach teleinformatycznych;
- *zagrożenia mające swoje odniesienie bezpośrednio do praw obywatelskich,* sprzedaż informacji czy przekazywanie podmiotom do tego nieuprawnionym[3].

F. Wołowski i J. Zawiła-Niedźwiecki zaprezentowali przykładowe kategorie [ISO/IEC TR 18044:2004], mogące zagrozić działalności przez organizację. Należy wskazać na potyczki, błędy ludzi, niepoprawne działanie systemu, jego nadmierne prze-

[1] Tamże.
[2] R. J. Sutton, *Bezpieczeństwo telekomunikacji*…dz. cyt., s. 17.
[3] P. Bączek, *Zagrożenia informacyjne a bezpieczeństwo państwa polskiego*, Wydawnictwo Adam Marszałek, Toruń 2006, s. 72-73.

ciążenie, utratę urządzenia, usługi, funkcjonalności. Te czynniki są najczęstszymi przyczynami mogącymi zagrozić organizacji. Jednakże nie należy zapominać o rzadszych aczkolwiek jakże powszechnych w społeczności działaniach powodujących załamanie prawidłowo funkcjonującego kanału przepływu informacji. Jest to m.in. dopuszczenie do sytuacji, w której doszło do naruszenia ustaleń związanych z bezpieczeństwem informacyjnym, odstępstwo od przyjętych zaleceń a w szczególności norm. Pojawić się może złe działanie sprzętu lub wadliwe oprogramowanie jak również niekontrolowanie zmiany systemu, odmowa obsługi i naruszenie systemu kontroli dostępu.

Często zdarza się zablokowanie zasobów wynikające z błędnej konfiguracji, niekompletności oprogramowania, otwieranie dodatkowych sekcji bez konkretnego powodu, wysyłanie wiadomości w błędnych formatach, nielegalne pozyskiwanie informacji czy kradzież i zniszczenie sprzętu, celowe i nieumyślne bądź zniszczenie go w trakcie pożaru lub zalania albo zbyt niska lub wysoka temperatura.

Najczęstszą przyczyną wystąpienia ataku w wyniku, którego dochodzi do naruszenia ochrony fizycznej i dostępu do informacji jest źle bądź słabo skonfigurowany system operacyjny. Szczególne przypadki powodujące dostęp do informacji osobom do tego nieuprawnionym to:

- pozyskiwanie haseł i wykorzystywanie plików w celu oszukania, przejęcia połączeń sieciowych;
- przepełnienie bufora w celu uzyskania przywilejów dodatkowych;
- spadek wydajności spowodowany zwiększająca się liczbą użytkowników;
- błędy, awarie sprzętu, ataki poprzez naruszenie integralności i dostępności;
- usuwanie plików, danych na nich zamieszczonych w wyniku włamania;
- ujawnienie pozyskanych informacji i wykorzystanie ich w prywatnych celach bez zgody drugiej strony[1].

Ważną kwestia są również ataki na zbiory danych mających stanowić o tajemnicy państwowej lub służbowej. Działania te maja na celu przejęcie kontroli nad chronionymi systemami i występują w sytuacji, gdy działania zmierzające do naruszenia ich bezpieczeństwa są celowe. Ataki zostały podzielone na dwie grupy:

- *pasywne*, charakteryzują się brakiem aktywnego oddziaływania na system (podsłuchy, podgląd, analiza ruchu w sieci);

[1] F. Wołowski, J. Zawiła-Niedźwiecki, *Bezpieczeństwo systemów informacyjnych. Praktyczny przewodnik zgodny z normami polskimi i międzynarodowymi*, Wydawnictwo edu-Libri, Kraków-Warszawa 2012, s. 140-142.

- *aktywne*, wynikają z aktywnego oddziaływania na system, pośrednio bądź bezpośrednio, polegają na modyfikowaniu strumienia danych, tworzeniu danych fałszywych[1]. W czasach teraźniejszych podstawą sprawnego osiągnięcia celu jest odnalezienie się i panowanie w przestrzeni internetowej. Taka moc pozwala na użycie środków walki a dopiero właśnie to umożliwia pozyskanie przewagi w konkretnym środowisku[2]. Na rysunku 3.1 został przedstawiony podział zagrożeń informacyjnych.

Rysunek 3.1. Podział zagrożeń informacyjnych

Źródło: Opracowanie własne na podstawie, P. Bączek, Zagrożenia informacyjne a bezpieczeństwo państwa polskiego, Wydawnictwo Adam Marszałek, Toruń 2006, s. 30

Zagrożenie bezpieczeństwa informacyjnego w opinii P. Bączka może mieć odwołanie do działalności człowieka czy chociażby organizacji:

- walka informacyjna;
- cyberterroryzm;
- zagrożenia asymetryczne;

[1] A. Żebrowski, W. Kwiatkowski, *Bezpieczeństwo informacji III Rzeczypospolitej*, Oficyna Wydawnicza ABRYS, Kraków 2000, s. 63.
[2] J. Wołejszo, B. Biernacik, *Wsparcie informatyczne działań połączonych*, „Kwartalnik BELLONA" nr 2/2015 (681), Warszawa 2015, s. 121.

- szpiegostwo;
- przestępstwa komputerowe;
- nieuprawnione ujawnienie informacji;
- korupcyjna;
- naruszenie przez władze praw obywatelskich;
- naruszenie prywatności;
- asymetria w międzynarodowej wymianie informacji pomiędzy państwami sojuszniczymi;
- działalność grup manipulujących przekazem informacyjnym;
- szybki i niekontrolowany rozwój nowoczesnych technologii bioinformatycznych[1].

A. Żebrowski poparł powyższą tezę odnoszącą się do opinii, iż źródłem zagrożenia bezpieczeństwa informacyjnego jest człowiek. Właśnie to człowiek może wykorzystywać techniki włamań do systemów informacyjnych, będących cennym źródłem informacji. Takie dane stanowią tajemnicę państwową, służbową. Powszechnymi przykładami takich technik są:

- celowe inicjowanie awarii, wywoływanie fałszywych alarmów;
- zmowa kilku osób, szantaż, korupcja;
- pozyskiwanie pozornie nieważnych informacji znajdujących się pod śmietnikami firmowymi;
- rozkodowywanie haseł dostępu, rozsyłanie do firm ankiet, zapytań pod pozorem prośby o wejście w mało znaczący link, wirusy, robaki, konie trojańskie;
- podsłuch sieciowy, atak słownikowy;
- wykorzystywanie luk w zabezpieczeniach dostępu do poczty elektronicznej, serwisu informacyjnego oraz techniki obchodzenia zabezpieczeń, programy wykorzystujące błędy w operacyjnych systemach jak i oprogramowaniu użytkowym;
- przechwytywanie otwartych połączeń sieciowych, kryptoanaliza zaszyfrowanych informacji[2].

Jednym z zagrożeń najważniejszych dotyczących bezpieczeństwa informacyjnego jest możliwość niekontrolowanego dostępu oraz ujawnienia informacji przez osoby

[1] P. Bączek, *Zagrożenia informacyjne a bezpieczeństwo…dz. cyt.*, s. 86-87.
[2] A. Żebrowski, W. Kwiatkowski, *Bezpieczeństwo informacji…dz. cyt.*, s. 73.

trzecie stanowiącej tajemnicę[1]. Wyciek informacji często następuje poprzez ukryte kanały komunikacji, czyli ścieżki, którymi nie przesyła się informacji w ramach normalnego przetwarzania[2].

W opinii A. Nowak i W. Scheffs, następują zdarzenia, które w związku z brakiem wiedzy oraz świadomości użytkowników prowadzą do utraty bądź ujawnienia informacji mających miano ważnych. Działania takie są niewłaściwe, nieodpowiedzialne polegające czasami na zapisywaniu na kartkach haseł do komputera, konta w takim miejscu gdzie jest łatwy dostęp osób trzecich. Kolejnym niewłaściwym działaniem, o którym warto wspomnieć jest sytuacja, w której są hasła do karty są na niej zapisywane, co ułatwia przestępcom działanie[3].

Najczęściej wyróżnianymi formami zagrożeń teleinformatycznych jest:

- aktywizm, działalność niedestrukcyjna w ramach, której Internet służy wsparciu nowej kampanii przestępczej,
- haking, uzyskanie nieautoryzowanego dostępu do danych użytkownika, przez osobę, która nie posiada uprawnień,
- cyberterroryzm, to dokonanie ataków przy pomocy technologii informacyjnej a jej nadrzędnym celem wyrządzenie szkody w odniesieniu do infrastruktury a pobudki tego czynu mogą być ideologiczne, polityczne,
- cyberprzestępczość, to najczęściej przestępczość komputerowa a polega ona na nielegalnym wykorzystaniu sieci, komputerów, Internetu do wszelkich czynów niedozwolonych,
- cyberszpiegostwo, ma miano aktywności ofensywnej celem jest kradzież poufnych informacji[4],
- skutki niekontrolowanego użycia Internetu w sferze psychicznej i społecznej[5].

Widać wyraźnie, ze podatność na zagrożenia bezpieczeństwa informacyjnego wynika z rozwoju sieci. Dzięki odpowiednim narzędziom oraz umiejętnościom każdy człowiek dysponuje nieograniczonym dostępem do informacji.

[1] Tamże, s. 61.
[2] F. Wołowski, J. Zawiła-Niedźwiecki, *Bezpieczeństwo systemów…dz. cyt.*, s. 276.
[3] A. Nowak, W. Scheffs, *Zarządzanie bezpieczeństwem…dz. cyt.*, s. 6.
[4] *Szeroko Bezpieczeństwo teleinformatyczne państwa,* red. M. Madej, M. Terlikowski, Polski Instytut Spraw Międzynarodowych, Warszawa 2009.
[5] *Szeroko Patologie w cyberprzestrzeni. Profilaktyka zagrożeń medialnych*, red. D. Morańska, Wydawnictwo Naukowe Wyższej Szkoły Biznesu, Dąbrowa Górnicza 2015.

Dostęp do sieci jest ogólnie dostępny, w związku z powyższym coraz częściej jest wykorzystywany przeciwko społeczeństwu[1]. Szczególnym wyzwaniem dla bezpieczeństwa Polski i innych państw wysokorozwiniętych będą negatywne oddziaływania w cyberprzestrzeni. Mogą one wynikać z nieumyślnego lub celowego działania człowieka bądź zakłóceń funkcjonowania infrastruktury teleinformatycznej[2]. Do lepszego zobrazowania koniecznym jest wyjaśnienie pojęcia, jakim jest cyberprzestrzeń.

Kierując się opiniami zawartymi w źródłach naukowych jest to przestrzeń cyfrowa, w której następuje przetwarzanie oraz wymiana informacji. Tworzą ją systemy informatyczne, sieci, istnieją również ścisłe powiązania pomiędzy nimi a użytkownikami[3]. Termin cyberprzestrzeń (ang. cyberspace) stworzył i upowszechnił w 1984 r. William Gibson, określił on cyberprzestrzeń, jako „konsensualną halucynację, doświadczaną każdego dnia przez miliardy uprawnionych użytkowników we wszystkich krajach"[4].

W literackim ujęciu określenie cyberprzestrzeni z dużą trudnością poddaje się naukowemu zdefiniowaniu, odpowiadając wymogom teorii zastosowania reguł semiotycznych oraz praw logiki formalnej w odniesieniu do działalności naukowej[5]. W powszechnie dostępnej literaturze określenie cyberprzestrzeni rozumiane jest, jako obszar, cyfrowa domena mająca służyć do wymiany informacji. Stanowi ją suma działań wykonywanych przez użytkowników[6].

W opinii P. Sienkiewicz i H. Świeboda, cyberprzestrzeń została ukształtowana przez procesy takie jak:

- konwergencji ICT, systemów telekomunikacyjnych, informatycznych, mediów elektronicznych;
- integracji podstawowych form prezentacji i przekazu informacji, który przyniósł multimedialność;
- integracji technosfery, który ukształtował globalną zintegrowaną platformę teleinformatyczną.

---

[1] M. Karatysz, *Zjawisko cyberprzestępczości a polityka cyberbezpieczeństwa w regulacjach prawnych Rady Europy, Unii Europejskiej i Polski,* Wydawnictwo Naukowe UAM, Poznań 2013, s. 140.
[2] *Strategia Rozwoju Systemu Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej 2022*, przyjęta uchwałą Rady Ministrów z dnia 9 kwietnia 2013 r., s. 33.
[3] J. Kowalewski, M. Kowalewski, *Cyberterroryzm szczególnym zagrożeniem bezpieczeństwa państwa, „Telekomunikacja i techniki informacyjne*", 1-2/2014, s. 24.
[4] W. Gibson, *Neuromancer*, Poznań 1999, s. 53.
[5] J. Janowski…dz. cyt.,http://www.bibliotekacyfrowa.pl/Content/46512/23_Jacek_Janowski.pdf, s. 311 [dostęp: 21.06.2022].
[6] J. Wasilewski, *Zarys definicji cyberprzestrzeni, [w:] Przegląd bezpieczeństwa narodowego*, red. B. Hołyst, Wydawnictwo ABW, Warszawa 2013, s. 231.

Cyberprzestrzeń jest obszarem kooperacji pozytywnej i negatywnej. Kooperacja pozytywna oznacza wzrost możliwości wszechstronnego zaspokojenia potrzeb społecznych, w tym potrzeby samorozwoju, samorealizacji we wszystkich dziedzinach życia.
W sferze edukacji dzięki zwiększonym i ułatwionym możliwościom korzystania z globalnych zasobów danych, informacji i wiedzy (Europejska Przestrzeń Edukacyjna).
W sferze ekonomii, poprzez rozwój „e-biznesu" oraz powstanie tzw. gospodarki opartej na wiedzy".

W sferze badań naukowych dzięki wzrostowi zasobów wiedzy i wspomagania badań (Europejska Przestrzeń Badawcza), jak również w sferach takich jak bezpieczeństwo, kultury i komunikacji. Dzięki zwiększonej sprawności służb nastąpił wzrost bezpieczeństwa obywateli, jednakże kosztem utraty części wolności, a dzięki niemal nieograniczonemu dostępowi do zasobów wirtualnej ikonosfery nastąpiła możliwość zaspokojenia potrzeby związanej ze sferą kulturową. Rozwój sieci komunikacji społecznej w skali globalnej prowadzi do rozwoju w sferze komunikacji. Negatywna strona oznacza, że cyberprzestrzeń stała się źródłem zagrożeń dla bezpieczeństwa zewnętrznego, międzynarodowego oraz wewnętrznego, narodowego.

Możemy mieć do czynienia z takimi zjawiskami jak:

- Cyberterroryzm są to działania terrorystyczne w cyberprzestrzeni;
- Cyberinwigilacja związana z wykorzystaniem cyberprzestrzeni w celach kontroli społecznej np. identyfikacja lokalizacji;
- Cyberprzestępstwa mają na celu wykorzystanie cyberprzestrzeni dla celów kryminalnych, zarówno przestępstw pospolitych jak i zorganizowanych;
- Cyberwojna nacechowana jest działaniami wojennymi przy wykorzystaniu cyberprzestrzeni[1]. W literaturze dokonuje się określenia cyberterroryzmu, jako broni masowego rażenia, która docelowo wraz z dalszym rozwojem będzie stawała się bardzo niebezpieczna[2]. Cyberprzestępstwo określane jest, jako czyn zabroniony a jego miejscem jest cyberprzestrzeń[3]. Barry Collin cyberterroryzm określił, jako przejście terroryzmu ze świata realnego do wirtualnego[4].

[1] P. Sienkiewicz, *Analiza systemowa zagrożeń…dz. cyt.*, s. 589. http://journals.bg.agh.edu.pl/AUTOMATYKA/2009-02/Auto46.pdf, s. 585. http://journals.bg.agh.edu.pl/AUTOMATYKA/2009-02/Auto46.pdf [dostęp: 25.11.2022].
[2] S. Wojciechowska-Filipek, Z. Ciekanowski, *Bezpieczeństwo informacyjne w cyberprzestrzeni jednostki - organizacji – państwa*, Wydawnictwo CeDeWu sp. z o.o., Warszawa 2016, s. 203.
[3] J. Kowalewski, M. Kowalewski, *Cyberterroryzm szczególnym…dz. cyt.* ,s. 24.
[4] W. L. Tafoya, Cyber Terror, „FBI Law Enforcement Bulletin", vol. 80, no. 11, 2011, s. 2. https://leb.fbi.gov/2011/november/leb-november-2011 [dostęp:17.12.2023].

Cyberterroryzm według Dorothy Denning jest zbieżnością cyberprzestrzeni oraz terroryzmu. Ma swoje odniesienie zarówno do bezprawnych ataków, gróźb i ataków na komputery, sieci i przechowywanych w nich informacji. Celem będzie zastraszenie lub zmuszenia rządu, decydentów, odwołując do wsparcia celów politycznych bądź społecznych. Atak powinien powodować znaczne straty lub takie skutki, które wywołują poczucie strachu, aby działania takie zostały zakwalifikowane, jako terroryzm informacyjny.

Działania, które prowadzą do śmierci bądź uszkodzenia ciała, eksplozje, a także poważne straty ekonomiczne mogą być tego przykładem. Ataki na infrastrukturę krytyczną mogą zostać uznane za akty cyberterroryzmu, jest to ocenione w zależności od wielkości wyrządzonych szkód [1]. W opinii T. Szubrychta cyberterroryzm dzieli się na trzy grupy. Po pierwsze pojęcia prezentowane w mediach, po drugie obowiązujące w gronie specjalistów a po trzecie definicje stworzone na użytek innych dziedzin działalności człowieka w dziedzinie informatyki[2]. M. Pollit uważa cyberterroryzm za zaplanowany i politycznie umotywowany atak przeciwko systemom, bazom danych czy programom komputerowym[3]. James A. Lewis rozpatruje cyberterroryzm, poprzez użycie sieci i narzędzi komputerowych w celu sparaliżowania działania narodowej infrastruktury krytycznej, czyli sieci transportowe, energetyczne, rządowe, poprzez zastraszenia, wymuszenia na rządzie czy populacji określonych zachowań zgodnych z wizją i potrzebą sprawcy tych działań[4].

Do przeciwstawnej formy, jaką jest cyberprzestępstwo zaliczyć należy cyberbezpieczeństwo mające swoje odniesienie do odporności systemów informacyjnych na działania mające związek z naruszeniem poufności, dostępności, integralności i autentyczności usług oraz przetwarzanych danych[5]. W literaturze można odnaleźć podstawowy podział cyberataków. Pierwszy znajduje swoje odzwierciedlenie tylko w cyberprzestrzeni

[1] D. Denning, *Testimony before the Special Oversight Panel on Terrorism Committee on Armed Services U.S. House of Representatives*, 2000, http://faculty.nps.edu/dedennin/publications/Testimony-Cyberterrorism2000.htm[(dostęp: 15.07.2022].
[2] T. Szubrycht, *Cyberterroryzm jako nowa forma zagrożenia terrorystycznego*, „Zeszyty Naukowe Akademii Marynarki Wojennej", nr 1, 2005, s. 17.
[3] M. M. Pollit, *Cyberterrorism – Fact or a Fancy?, [w:] Focus on Terrorism*, ed. E.V. Lin-den, New York 2007, s. 67, https://books.google.pl/books?id=wl=-D 42 sYMDIC&pg=P65 A&dq-Cyberterrorism+%E2%80%93+Fact+or+Fancy&hl=pl&sa=X&redir_esc=y#v=onepage&q=Cyberterrorism%20%E2%80%93%20Fact%20or%20Fancy&f=false [dostęp: 25.12.2023].
[4] J. A. Lewis, *Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats*, Center for Strategic & International Studies, 2002, s. 1, http://csis.org/files/media/csis/pubs/021101_risks_of_cyberterror.pdf [dostęp: 25.12.2023].
[5] Ustawa z dnia 5 lipca 2018r. *o krajowym systemie cyberbezpieczeństwa*, Dz.U. 2018 poz. 1560, s. 1.

drugi to ataki na systemy informacyjne. Wyróżnić można wiele metod ataków i z postępem technologii coraz to nowsze działania są wykorzystywane.

Do takich działań zaliczyć należy ataki z udziałem:

- konia trojańskiego, czyli programu wykonującego działania niepożądane takie jak usuwanie plików, formatowanie dysków bądź przesyłanie danych z komputera lub przenośnika do osób nieuprawnionych. Wszystkie te działania odbywają się bez wiedzy i świadomości użytkownika;
- bomby logicznej, czyli pewnego rodzaj wirusa komputerowego, którego uruchomienie następuje przez konkretne zdarzenie, wpisanie komendy, uruchomienie programu;
- ataki wykorzystujące złośliwe oprogramowanie typu, wirusy, robaki, bakterie, których celem jest samoistne zarażenie określonych obszarów komputera, doprowadzając do złego, wolnego jego funkcjonowania, generując ogromne straty;
- tylne drzwi, czyli backdoor, oprogramowanie wykorzystywane do włamania się do komputerów użytkowników z nich korzystających i tworzone w celu naprawiania błędów w oprogramowaniu;
- denial of service (DoS), distributed denial of service (DDos), działania polegające na zablokowaniu poprawnego funkcjonowania konkretnego serwisu sieciowego, przesyłanie potężnego pakietu danych z różnych źródeł, co w konsekwencji spowoduje zawieszenie komputera;
- hijacking, swoje działanie opiera na przechwyceniu transmisji odbywającej się między dwoma systemami a następnie wykorzystaniu jej do celów własnych;
- sniffing, programy wyłapujące w sieci wiadomości i zapisujące je na dysk w celu późniejszego ich przetworzenia oraz wyłapania haseł bądź danych osobowych, innymi słowy działanie to polega na podsłuchiwaniu, tropieniu ruchu w sieci;
- spoofing, w celu destabilizacji danego systemu, podszywanie się pod użytkowników;
- chipping, umieszczanie chipów w komputerach, zawierających oprogramowanie dające dostęp do systemu, w którym zostały zainstalowane[1].

Cyberterroryzm w dobie tak szybkiego rozwoju systemów informatycznych stanowi duże zagrożenie dla Państwa. Z raportów analityków badających tą dziedzinę wynika, ze ponad osiemdziesiąt procent systemów informatycznych administracji publicznej w Polsce jest zagrożonych atakami miedzy innymi ze strony hakerów. Dla Polski takimi

[1] A. Bógdał-Brzezińska, M. F. Gawrycki, *Cyberterroryzm i problemy bezpieczeństwa informacyjnego we współczesnym świecie*, Oficyna Wydawnicza ASPRA-JR, Warszawa 2003, s. 138–154.

zagrożeniami mogą być oddziaływania w cyberprzestrzeni skierowane na systemy i sieci teleinformatyczne infrastruktury krytycznej[1].

Studium przypadku:

W mediach w połowie grudnia roku 2014 pojawiły się informacje o zanotowanych włamaniach do systemów komputerowych operatora południowokoreańskich elektrowni jądrowych. Żądaniem hakera było włączenie reaktorów nuklearnych. Mimo zapewnieniom władz Korei Południowej o fakcie potwierdzenia bezpieczeństwa reaktorów, otrzymana wiadomość zaniepokoiła cały świat. W roku 2013, belgijski operator telekomunikacyjny Belgacom ogłosił, iż w jego systemach komputerowych zostało znalezione złośliwe oprogramowanie, zdolne do mutacji i wyjątkowo skomplikowane do usunięcia. Dochodzenie odnośnie zaistniałej sprawy prowadziła belgijska prokuratura generalna, która ustaliła, że osoby trzecie posiadały dużą wiedzę ekspercką i dysponowali dużymi środkami finansowymi. W Belgii mają siedziby takie organizacje międzynarodowe jak NATO czy Unia Europejska w związku z powyższym jest to kraj szczególnie narażony na działania terrorystyczne, szpiegowskie, cyberterrorystyczne. Estonia w roku 2007 odnotowała falę ataków cybernetycznych. W historii był to pierwszy przypadek, kiedy niepodległe państwo było ofiarą cybernetycznego ataku na tak ogromną skalę. Serwery, strony internetowe, systemy informatyczne parlamentu estońskiego, rządowych agend, mediów i banków zostały zaatakowane przez hakerów. Początkowo myślano, że te działania były na zlecenie rosyjskiego rządu. Ostatecznie jednak okazało się, że te działania zostały zainicjowane przez 20-letniego studenta Estonii. Każde z działań pokazuje jak ataki cybernetyczne mogą stanowić dla funkcjonowania państwa ogromne niebezpieczeństwo[2].

Kolejnym przykładem może być włamanie się hakerów na jedną ze stron rządowych USA. Cyberprzestępcy zakomunikowali, że są obywatelami Iranu a atak jest zemstą za śmierć generała Kasema Sulejmaniego. Działania hakerskie związane były z opublikowaniem grafiki przedstawiającej Donalda Trumpa uderzonego pięścią w twarz. Obraz

[1] M. Wrzosek, *Zagrożenia bezpieczeństwa Polski. Teoria i praktyka*, „Kwartalnik BELLONA", Rocznik XCV (VII), nr 2/2013 (673) Warszawa, s. 39.
[2] https://zpe.gov.pl/a/cyberterroryzm/D4HRR86ro, [dostęp: 28.12.2023].

ten został zamieszczony na stronie FDLP, w miejscu gdzie udostępniane są zasoby rządowych publikacji[1]. Cyberatak wymierzony w wojska USA w Polsce. 20.01.2020 roku, hakerzy podszyli się pod znany portal". Wiadomości mailowe wysłane były przez osoby podszywające się pod pracowników Grupy Defence24 i trafiły do wybranych instytucji. Wysłane e-maile zawierały prośbę o komentarz w sprawie nieprawdziwej informacji o zorganizowaniu przez Urząd Miejski i burmistrza Orzysza marszu „Nie dla wojsk USA w Polsce!", a także link do artykułu na portalu „Tygodnik Działdowski". Załączony link mógł rozsyłać złośliwe oprogramowanie[2]. Rozwój i powszechne zastosowanie informatyki mające swoje odzwierciedlenie w różnych sektorach gospodarki przyczyniło się do dużej technologicznej zależności biznesu od komputerów. Szybko ewoluująca technologia informatyczna obok masy korzyści generuje jakże poważne wyzwania.

Ze wzrostem liczby urządzeń końcowych, zwiększa się ilość środków, jakie trzeba posiadać na ich zabezpieczenie. Jak również wraz ze wzrostem liczby posiadanych danych przesyłanych nowoczesnymi, cyfrowymi środkami komunikacji, tym większe jest znaczenie ochrony danych w postaci mechanizmów backupu i odzyskiwania. W opinii eksperta ds. cybernetycznych w Allianz Global Corporate & Specialty S. Gettingera, firmy stają przed wyzwaniem związanym z droższymi i większymi naruszeniami danych, wzrostem liczby oprogramowania ransomware i incydentami fałszowania. *Incydenty stają się coraz bardziej szkodliwe, coraz częściej atakując duże firmy wyrafinowanymi metodami i wymuszeniami. Pięć lat temu typowy popyt na oprogramowanie ransomware wyniósłby dziesiątki tysięcy dolarów. Teraz można to liczyć w milionach.* M. Stanisławski z Deputy Global Head of Cyber w AGCS dodaje, że Straty mogą być też wynikiem niedostępności krytycznych danych, systemów lub technologii, zarówno z powodu usterki technicznej, jak i cyberataku.

W związku z powyższym szkolenia pracowników stają się szczególnie ważną potrzebą w kontekście ilości posiadanych i obsługiwanych urządzeń. Pracownicy często korzystają z prywatnych urządzeń w celach służbowych za przyzwoleniem pracodawców. Umożliwienie korzystania z własnych sprzętów dla wielu organizacji jest korzystne nawet ze względów ekonomicznych, czyli zwiększenie wydajności pracownika oraz obni-

[1] https://www.fakt.pl/wydarzenia/swiat/hakerzy-przejeli-rzadowa-strone-usa-groza-donaldowi-trumpowi/876len6 [dostęp: 02.01.2024].
[2] https://www.tvp.info/46280362/cyberatak-wymierzony-w-wojska-usa-w-polsce-hakerzy-podszyli-sie-pod-znany-portal [dostęp: 02.01.2024].

żenie kosztów eksploatacji. Nie zwraca się uwagi na fakt, że takie urządzenia mają zwykle gorsze oprogramowania i są słabiej zabezpieczone. Dzięki temu hakerom jest łatwiej włamać się do takiego prywatnego urządzenia. W takich sytuacjach firmy jednak będą musiały pochylić się nad poprawą polityki bezpieczeństwa w firmach poprzez na przykład wprowadzenie nowych zasad i ściśle je przestrzegać[1]. Aspektem problematycznym są sztuczne systemy informacyjno-sterujące, będące wytworem człowieka. L. Ciborowski zauważa, że w odróżnieniu od systemu naturalnego nigdy nie były, nie są i najprawdopodobniej nigdy nie będą idealne.

Rozwiązania strukturalne i organizacyjne, hierarchiczne, funkcjonalne, informacyjne i techniczne, w nich stosowane, tworzone są zawsze tylko w aspekcie chwilowych, dających się przewidywać potrzeb ich twórców na miarę zdobytej przez nich wiedzy i fizycznych możliwości jej materializowania w konkretnych rozwiązaniach. Umysł ludzi przekształca zarejestrowane dane w odpowiednie sygnały dla organizmu. W rzeczywistości wszystkie elementy systemu informacyjno-sterującego począwszy od zbiorów danych odbierających, a skończywszy na ostatnim układzie odbierających funkcjonują w otoczeniu ciągłych zakłóceń. W dużej mierze narażone są na negatywne oddziaływanie losowe, jak i mogą być obiektami działania zakłóceń generowanych celowo. L. Ciborowski podjął próbę zdefiniowania walki informacyjnej, którą stanowią działania kooperacji negatywnej wzajemnej, w których cel destrukcyjnego oddziaływania skoncentrowany jest na systemach informacyjno-sterujących przeciwnych sobie stron.

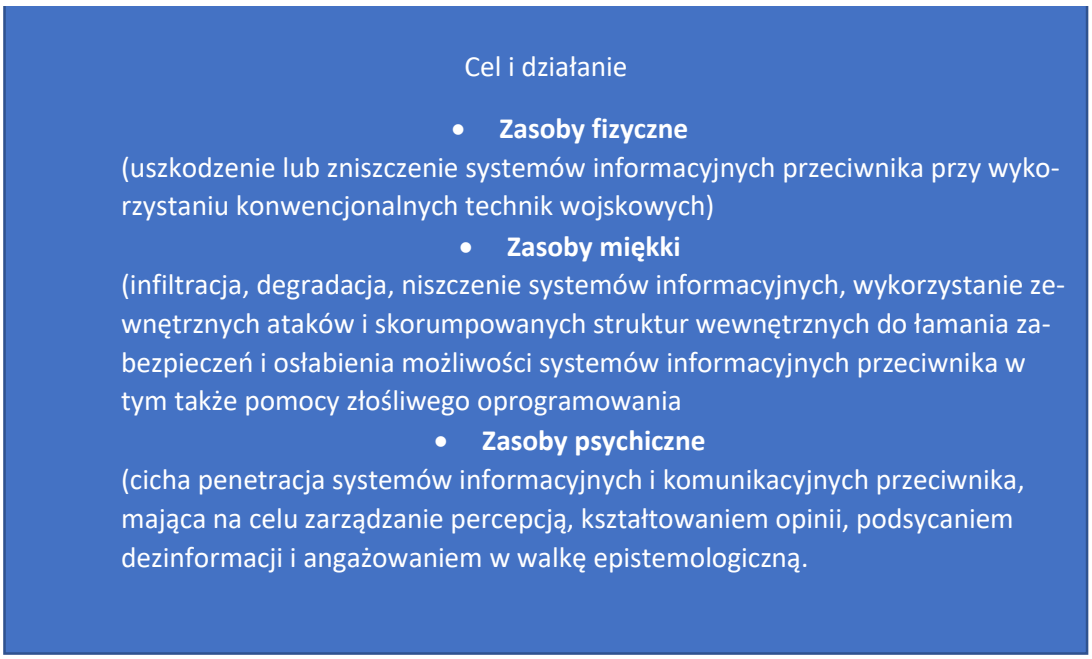
Informacja jest postrzegana, jako coś niematerialnego, na co nie można oddziaływać środkami materialnymi. Charakter walki informacyjnej lokuje ją w grupie walk niezbrojnych. Zawsze prowadzona jest wspólnie z innymi walkami politycznymi, walkami ekonomicznymi, walkami zbrojnymi, walkami sportowymi, walkami ideologicznymi itp.[2] Stanowisko jakże podobne przyjął K. Liedel, definiując walkę informacyjną, jako istniejący konflikt mający swoje rozstrzygnięcie za pomocą informacji traktowanej, jako broń skierowana przeciwko zasobom informacyjnym przeciwnej strony przy jednoczesnej obronie własnych zasobów informacyjnych[3].

Elementami walki informacyjnej jest, destrukcja fizyczna, operacje psychologiczne bezpieczeństwa, sabotaż, walka elektroniczna. Narzędzia wykorzystywane do

[1] https://www.computerworld.pl/news/Cyberbezpieczenstwo-wsrod-najwiekszych-ryzyk-biznesowych-w-2020- r,417286.html?utm_source=news&utm_campaign=polecane&utm_medium=tags [dostęp: 25.012.2023].
[2] L. Ciborowski, *Walka informacyjna…dz. cyt.*, s. 65-87.
[3] K. Liedel, P. Piasecka, T. R. Aleksandrowicz, *Analiza…dz. cyt.,* s. 32.

walki to, dyplomacja, propaganda, działania na poziomie wpływania na procesy kulturowe i polityczne, kampanie psychologiczne. Za pomocą mediów często dochodzi do manipulacji i rozszerzonej dezinformacji, która prowadzi do zagubienia, oszołomienia społeczeństwa. Ostatnim narzędziem, które zostanie wskazane będzie infiltracja sieci komputerowych oraz baz danych[1]. Na rysunku 3.2. zostały przedstawione trzy płaszczyzny celów i związanych z nimi działań.

Rysunek 3.2. Wojna informacyjna z podziałem na cel i działanie



Źródło: Opracowanie własne na podstawie, B. Cronin, H. Crawford, Information Warfare: Its Application in Military and Civilian Contexts, *„The Information Society”,* Vol. 15, No. 4, Indiana University, Bloomington 1999, s. 258

Zgodnie z definicją Kolegium Szefów Połączonych, walka informacyjna jest działaniem podjętym w celu osiągnięcia informacyjnej dominacji poprzez wpływ na informację przeciwnika jego procesy oparte na informacji, systemy informacyjne i sieci komputerowe[2]. Terroryzm to proces komunikacji oparty na przemocy, wywieraniu wpływu i manipulacji. Chęć osiągnięcia własnych celów popycha terrorystów do przyciągnięcia uwagi na opinię publiczną, wykorzystując istniejące kanały komunikacji, jakimi jest te-

[1] JP3-13 Joint Doctrine for Information Operations, Department of Defense, Washington 1998, [w:] T. R. Aleksandrowicz, *Podstawy walki informacyjnej*, Warszawa 2016, s. 133.
[2] K. Giles, *Handbook of Russian Information Warfare*, NATO 2016.

lewizja, prasa bądź stworzenie własnych kanałów służących do przekazywania informacji a narzędziem do tego może być Internet[1]. Według K. Liedela działania nacechowane walkami informacyjnymi noszą miano terroryzmu.

Większość definicji mających miano terroryzmu zawiera takie czynniki jak przemoc, rozgłos, demonstracja siły, strach wywołany wśród społeczeństwa[2]. T. Szubrycht twierdzi, iż *konflikt zbrojny jest asymetryczny i jest wówczas, kiedy państwo i jego siły zbrojne konfrontowane są z przeciwnikiem, którego cele, organizacja, ośrodki walki oraz metody działania nie mieszczą się w konwencjonalnym pojęciu wojny*[3]. Zagrożenia asymetryczne polegają przede wszystkim na strategii, w której państwo atakujące posiada przewagę. W takich konfliktach odmiennie postrzegany jest również przeciwnik. Odpowiednia taktyka powoduje, że przestaje być znany a staje się rozproszony, nieznany i w ten sposób niwelujący możliwość odwetu[4]. Globalizacja informacji jak również zasobów teleinformatycznych objęła zasięgiem cały świat, jednak rozwój cyfryzacji przebiega w sposób indywidualny w zależności od poziomu społecznej świadomości, zamożności, nauki, potrzeb, polityki[5].

Powszechnemu użyciu informacji, danych towarzyszą organizacje, które głęboko zmieniają życie, pracę i społeczeństwo[6]. W opinii P. Sienkiewicza społeczeństwo informacyjne to system społeczny, który ukształtował się w procesie modernizacji a systemy informacyjne i zasoby informacyjne determinują społeczną strukturę zatrudnienia oraz wzrost zamożności społeczeństwa. Uważa również, że społeczeństwo informacyjne charakteryzuje się:

- wysokim tempem rozwoju sieci komunikacji społecznej i modernizacji struktury informacyjnej;
- powstaniem „nowej gospodarki", jako rezultatem interakcji techniki (głównie IT), gospodarki i społeczeństwa;

[1] K. Liedel, *Transsektorowe obszary bezpieczeństwa narodowego*, Difin, Warszawa 2011, s. 98.
[2] Tamże, s. 97.
[3] T. Szubrycht, *Analiza podobieństw operacji militarnych innych niż wojna oraz działań pozwalających zminimalizowania zagrożenia asymetryczne*, „Zeszyty Naukowe Akademii Marynarki Wojennej", nr 1 (164), 2006, s. 145.
[4] M. Madej, *Terroryzm i inne zagrożenia asymetryczne w świetle współczesnego pojmowania bezpieczeństwa narodowego i międzynarodowego – próba teoretycznej konceptualizacji, [w:] Porządek międzynarodowy u progu XXI wieku*, red. R. Kuźniar, Wydawnictwo UW, Warszawa 2005, s. 23.
[5] M. Majchrzak, *Wpływ rozwiązań informacyjnych…dz. cyt.*, s. 93.
[6] L. Soete, *Building the Information Society for Ali Us. Finał Report of the High Level Export* Group (Bruksela: 1997) - wg [DÜKT2002], s. 100.

- bezpieczeństwem informacyjnym, jako istotnym elementem bezpieczeństwa społeczeństwa (w dziedzinie obronności powstaniem koncepcji Information Warfare i Cyberwar);
- dominacją sektora usług w społecznej strukturze zatrudnienia wraz ze stałym rozwojem (ilościowym i jakościowym) usług informacyjnych;
- nadaniem zasobom informacyjnym rangi zasobów strategicznych;
- globalizacją systemów informacyjnych (Internetu), jako czynnika globalizacji gospodarczej;
- wysokim wpływem IT i mediów elektronicznych na zmiany zachowań społecznych (powstanie fenomenu Cyberculture)[1].

M. Bangemann uważa, iż szeroka dostępność nowych narzędzi i usług informacji doprowadzi do stworzenia nowych możliwości budowy zrównoważonego społeczeństwa i poprawi indywidualnie osiągnięcia. Społeczeństwo informacji posiada potencjał polepszenia, jakości życia obywateli Europy, sprawności naszej społecznej i ekonomicznej organizacji oraz umocnienia spójności[2]. Ciągłe wdrażanie i otaczanie człowieka informacją oraz zasobami teleinformatycznymi przybrało postać zjawiska powszechnego, które uwarunkowuje jego procesy myślowe, dając możliwość zachowania łączności z bliższym i dalszym otoczeniem. Obserwacja tych zmian stała się przyczynkiem do podjęcia próby zdefiniowania społeczności wykazującej symptomy uwarunkowania, zależności i podatności na technologie informacyjne i komunikacyjne. Masuda przewidywał, że cywilizacja na przełomie XX i XXI wieku, nie będzie cywilizacją materialną, symbolizowaną przez ogromne konstrukcje, będzie natomiast cywilizacją tzw. *niewidoczną* – informacyjną[3]. W owej koncepcji planu zostały uwzględnione priorytety takie jak:

- racjonalizacja działań administracji;
- utworzenie krajowej sieci informacyjnej;
- system ochrony środowiska;
- modernizacja kanałów dystrybucyjnych;
- modernizacja ochrony zdrowia;

[1] P. Sienkiewicz, *Teoria rozwoju społeczeństwa informacyjnego, [w:] Polskie doświadczenia w kształtowaniu społeczeństwa informacyjnego. Dylematy cywilizacyjno-kulturowe*, red. L. H. Haber, Akademia Górniczo-Hutnicza, Kraków 2002, s. 506-507.
[2] M. Bangemann, *Europa i społeczeństwo globalnej informacji. Zalecenia dla Rady Europejskiej,* Bruksela 1994 kbn.icm.edu.pl/gsi/raport.html [dostęp: 05.01.2024].
[3] P. Sienkiewicz, *Analiza systemowa rozwoju społeczeństwa informacyjnego, [w:] Rewolucja informacyjna i społeczeństwo,* red. L. W. Zacher, Transformacje, Warszawa 1997, s. 7.

- informatyczne ukierunkowanie wykształcenia;
- rozwój współpracy międzynarodowej w dziedzinie informacji;
- rozpowszechnianie domowych urządzeń końcowych;
- skomputeryzowanie systemu komunikacyjnego;
- podniesienie systemów informacyjnych dla celów zarządzania na wyższym poziomie[1].

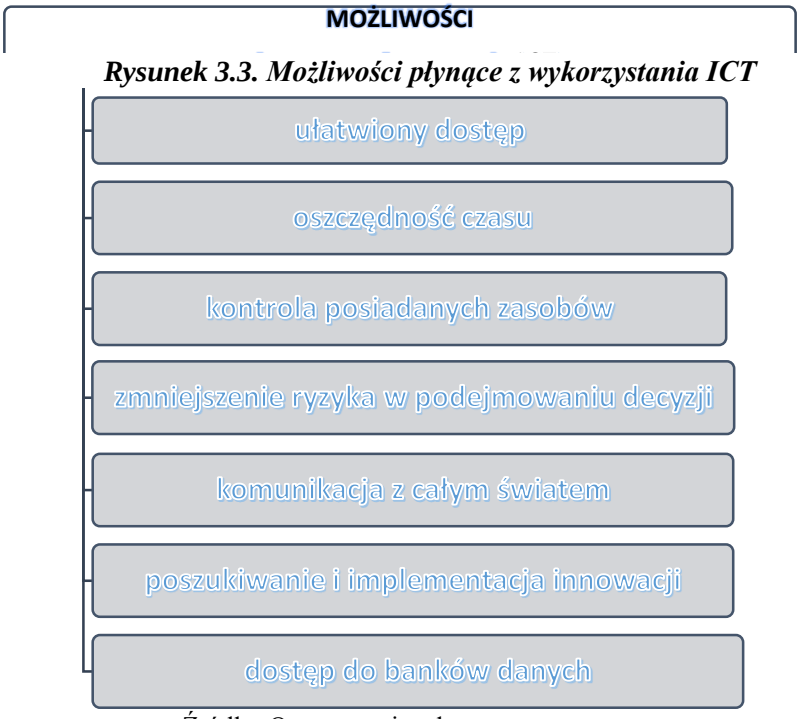
Nieodzowna chęć kontroli przez ograny międzynarodowe ekspansji społeczeństwa informacyjnego, stała się bodźcem do opracowania spójnych w skali międzynarodowej definicji i metodologii dostarczania porównywalnych danych. Miły one dotyczyć różnych aspektów społeczeństwa informacyjnego. W odniesieniu do źródeł, rozwój międzynarodowej statystyki społeczeństwa informacyjnego został zapoczątkowany przez Organizację Współpracy Gospodarczej i Rozwoju OECD w 1997 r., kiedy powołana została specjalna Grupa Robocza ds. Wskaźników Społeczeństwa Informacyjnego (Working Party for Indicators on Information Society – WPIIS)[2]. Tak czeto przywoływany inteligentny rozwój oznacza zwiększenie roli wiedzy
i innowacji, jako sił napędowych przyszłego rozwoju. Jednakże i tu należy sprostać pewnym wymogom takim jak podniesienie, jakości edukacji, poprawy wyników działalności badawczej, wspierania transferu innowacji i wiedzy w Unii.

Ważną kwestię pełni także maksymalne wykorzystanie technologii informacyjno-komunikacyjnych, a także zadbanie o to, aby innowacyjne pomysły miały swoje ujście w tworzeniu nowych produktów i usług. Działania te przyczyniłyby się do zwiększenia i tworzenia nowych miejsc pracy. Jednak, aby doszło do realizacji tego projektu nieodzowne są również elementy takie jak przedsiębiorczość, środki finansowe, uwzględnienie potrzeb użytkowników oraz możliwości rozwoju przez rynek oferowanych[3].

Człowiek w XXI w. stał się jednym z ogniw transformacji cyfrowej. Rozwój cyfryzacji spowodował, że coraz trudniej jest się wyzwolić od Internetu, komputerów, telefonów czy innych złożonych systemów i technologii, które stały się częścią jego codziennych spraw. Młodzież już od najmłodszych lat ma styczność z urządzeniami, które są ogólnodostępne w związku z rozwojem cyfryzacji. Dostęp do informacji dotyczących

[1] T. R. Aleksandrowicz, *Podstawy walki informacyjnej. Bezpieczeństwo dziś i jutro, EDO*, Warszawa 2016, s. 23.
[2] M. Goliński, *Społeczeństwo informacyjne - geneza koncepcji i problematyka pomiaru*, SGH - Oficyna Wydawnicza, Warszawa 2011, s. 11.
[3] *Komunikat Komisji Europa 2020. Strategia na rzecz inteligentnego i zrównoważonego rozwoju sprzyjającego włączeniu społecznemu, KE*, Bruksela 2010, s. 13-14.

państwa, organizacji gospodarczych, powoduje wzrost podmiotowości jak i świadomości społecznej. Tym samym zwiększa się zdolność sprawcza grup społecznych oraz poszczególnych jednostek[1]. Na rysunku 3.3 zostały przedstawione możliwości płynące z wykorzystania ICT.



Rysunek 3.3. Możliwości płynące z wykorzystania ICT

Źródło: Opracowanie własne

Społeczeństwo, które jest otwarte na zgłębiane wiedzy oraz pomnażanie posiadanego kapitału intelektualnego i materialnego dzięki wykorzystaniu cyfrowych narzędzi ma szersze możliwości w porównaniu ze społeczeństwem, które w jakimś sensie unika technologii. Takie sytuacje często wiążą się z brakiem pewności w siebie, obawą przed pomyłką. Różnorodność programów komputerowych, narzędzi służących społeczeństwu oraz wiedzy w odkrywaniu nowych obszarów nauki i poszukiwaniu informacji stwarzają możliwość rozwoju. Dają także szansę na doskonalenia kompetencji informatycznych. Obserwowana zachowawczość bardzo często wynika z indywidualnych uprzedzeń jednostki do innowacji oraz zmian, jakie wnosi ze sobą ICT.

Współczesnym niebezpieczeństwem dla społeczeństwa informacyjnego jest cyberprzestępczość. Zagrożone są w niej nie tylko zasoby w wymiarze materialnym, jak

[1] T. R. Aleksandrowicz…dz. cyt.., s. 49.

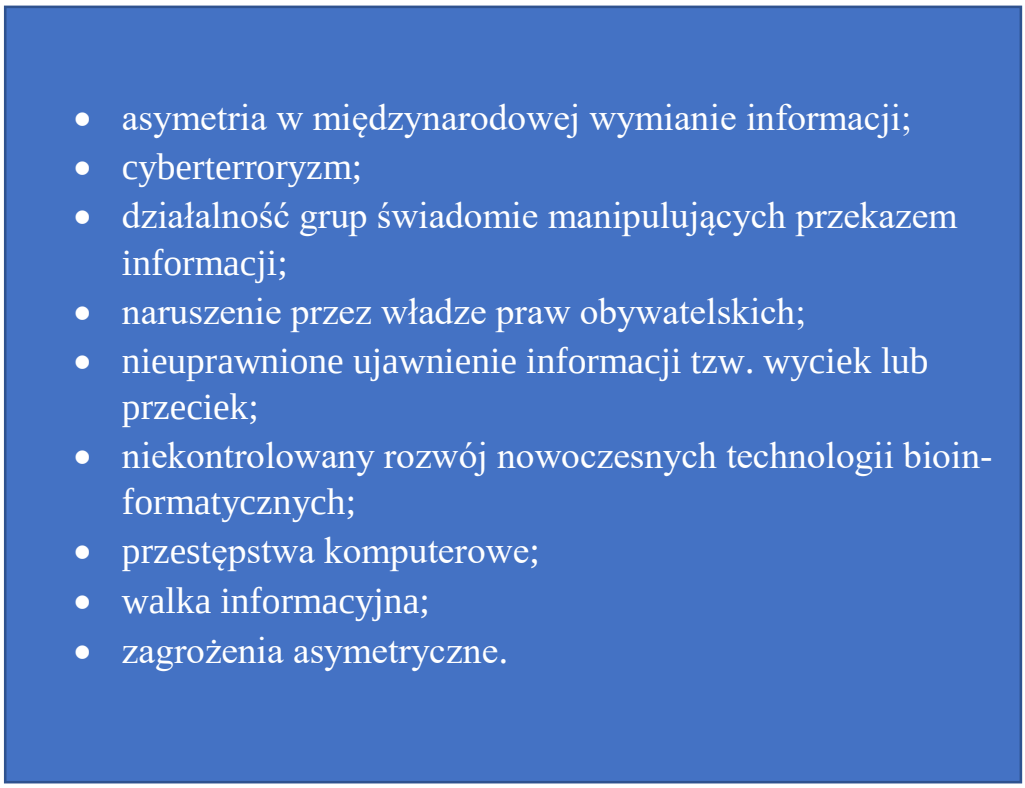
również te w wymiarze niematerialnym. Wynika to z faktu, że technologie komunikacyjne i informacyjne są aktywami niezwykle pożądanymi, zwłaszcza dla środowisk przestępczych, jak i wywiadowczych. Częste ograniczenia czasowe, jakie można zaobserwować wśród społeczeństwa informacyjnego doprowadzają do wyeliminowania bezpośredniego kontaktu oraz minimalizowania komunikacji werbalnej i niewerbalnej. Zaburzenia rozwoju wynikają z braku realnego, obustronnego kontaktu jednostki.

Olbrzymim niebezpieczeństwem zarówno dla interesów jednostki, jak i ogółu jest wykorzystanie narzędzi hackerskich do przejmowania systemów informatycznych, kont, wpływania na gospodarkę, politykę, obronność państwa. Środowisko hackerskie prześciga się w łamaniu zabezpieczeń systemów informacyjnych. Dla środowisk artystycznych, naukowych, dostrzegalnym problemem jest zawłaszczanie własności intelektualnej poprzez łatwy dostęp do prac autorskich a w przyszłości w związku z jeszcze szerszym i szybkim rozwojem technologii dojdzie do sytuacji, że prace będą pisane dzięki sztucznej inteligencji, co będzie miało swoje odzwierciedlenie w młodym społeczeństwie a autentyczność takiego wypracowania będzie ciężka do zweryfikowania. Formą dezintegracji lub destrukcji informatycznej mogą być wirusy komputerowe, bomby logiczne i konie trojańskie.

Różnicą jest fakt, iż bombę logiczną podkłada ktoś z wewnątrz, zaś koń trojański może być przesłany z zewnątrz, np. przez konkurencję, osoby nieprzychylne, zazdrosne. Znacznie mniej wyszukane są fizyczne czynniki destrukcyjne w rodzaju ładunków wybuchowych niszczących instalacje komputerowe. Z wyjątkiem wirusów komputerowych, w tej grupie zagrożeń występują przede wszystkim tradycyjne czynniki zagrożeń, dobrze znane i długo jeszcze mogące występować, a zaliczane do pospolitych przestępstw komputerowych, wymierzonych przeciw technice komputerowej.

Zagrożeniem jest również infiltracja, czyli działania osób nieupoważnionych mające na celu przenikanie do różnych elementów systemu informatycznego lub sieci telekomunikacyjnej[1]. Zagrożenia są inicjowane przez człowieka i jeżeli urządzenia, komputery są użytkowane świadomie to ryzyko zagrożeń ulega znacznej minimalizacji. Jeżeli zaś wykonywane działania mają miano celowych to wówczas zagrożenie wzrasta[2]. Poniżej na rysunku 3.4 zostały wskazane działania przyczyniające się do wywołania zagrożenia.

Rysunek 3.4. Działania przyczyniające się do wywołania zagrożenia



Źródło: Opracowanie własne

Wskazane powyżej zagrożenia mogą ingerować w systemy informacyjne jednostek organizacyjnych jak również osób fizycznych. Zależeć będzie tylko, co lub kto ma być celem działań przestępczych.

[1] T. Goban-Klas, P. Sienkiewicz, *Społeczeństwo informacyjne…dz. cyt.,* s. 67-69.
[2] P. Bączek, *Zagrożenia informacyjne a bezpieczeństwo państwa polskiego,* Wydawnictwo Adam Marszałek, Toruń 2006, s. 86-87.

3.2. Aspekty bezpieczeństwa systemu informacyjnego – strategia

Bezpieczeństwo postrzegane przez pryzmat danej jednostki i związane z realizacją potrzeby niższego rzędu zgodnie z opracowaną przez siebie hierarchią potrzeb (piramida) A. Maslowa. Przepływ informacji w organizacji charakteryzuje się złożonością i koniecznym jest rozpatrywanie jej w kontekście jej wejścia i wyjścia z obiegu w danej organizacji. Należy uwzględnić otoczenie bliższe i dalsze, gdzie podlega transformacji. Uznanie informacji za kluczowy element przewagi stanowi immamentną cechę współczesnych konfliktów, w których informacja jest wykorzystywana zarówno, jako broń, jak i traktowana, jako cel.

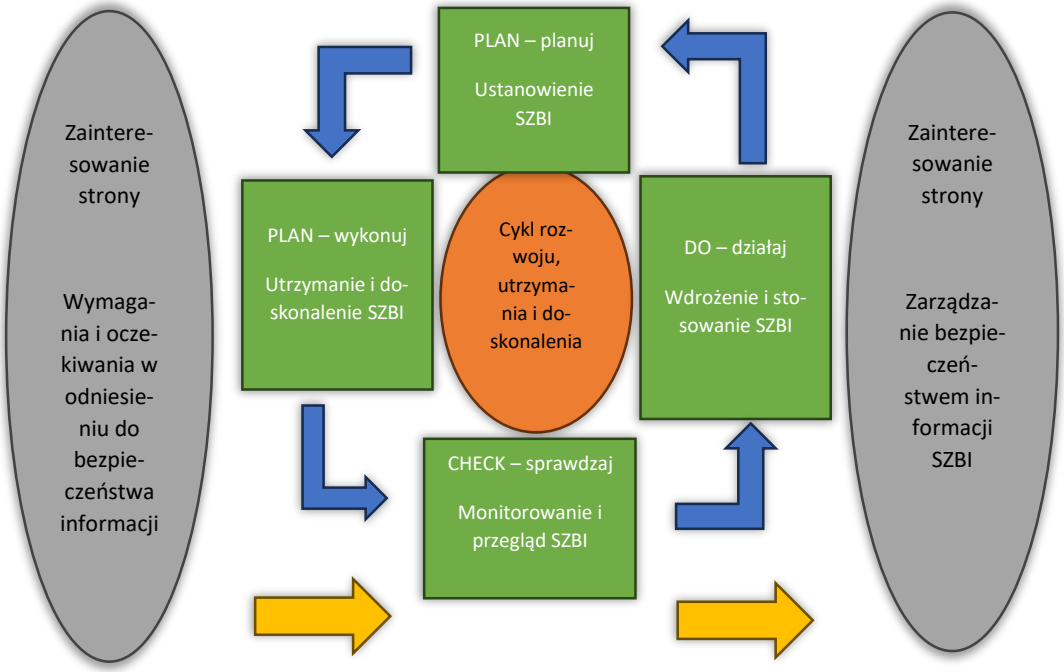
Teoretycy wskazują nawet na konieczność traktowania sfery informacyjnej, jako nowoczesnego środka walki[1]. W odniesieniu do PN-ISO/IEC 17799: 2007 bezpieczeństwo informacji definiowane jest, jako ochrona jej przed wszelkimi zagrożeniami w celu zapewnienia ciągłości działań, minimalizacji ryzyka niepowodzenia i maksymalizacji zwrotu z inwestycji i możliwości biznesowych[2]. Norma Polska pokazuje, iż bezpieczeństwo informacji stanowi o równowadze organizacji, jej rozwoju w otoczeniu wolnym od zagrożeń. W normie PN-ISO/IEC 27001:2017-06 Technika informatyczna - Techniki bezpieczeństwa - Systemy zarządzania bezpieczeństwem informacji - Wymagania ISO 27001 pod pojęciem bezpieczeństwa informacji kryje się zachowanie poufności, integralności i dostępności informacji; dodatkowo mogą być brane inne własności takie jak autentyczność, niezaprzeczalność i niezawodność.[3]

Polska Norma ISO/IEC 27001:2017-06 nakazuje zastosowanie podejścia procesowego dla ustanawiania, wdrażania, eksploatacji, monitorowania, przeglądu, utrzymywania i doskonalenia Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) w organizacji. Norma ta wskazuje model cyklu doskonalenia „Planuj – Wykonuj – Sprawdzaj – Działaj" (PDCA)[4], mający swoje odniesienie w systemie zarządzania bezpieczeństwem informacji (SZBI). Rysunek 3.5 przedstawia, w jaki sposób SZBI przyjmuje wymagania bezpieczeństwa informacji jak i oczekiwania zintegrowanych stron, jako wejściową wartość i poprzez działania oraz procesy dostarcza wartości wyjściowych bezpieczeństwa informacji, które spełniają te oczekiwania jak również wymagania[5].

---

[1] B. Balcerowicz, *Siły zbrojne w stanie…dz. cyt.*, s. 218.
[2] PN-ISO/IEC 17799: 2007, s. 9.
[3] PN-ISO/IEC 17799: 2007, s. 9.
[4] Plan–Do–Check–Act – koncepcja zaproponowana w ramach teorii zarządzania przez jakość Total Quality Managment (TQM) przez amerykańskiego naukowca i menedżera W. E. Deminga.
[5] F. Wołowski, J. Zawiła-Niedźwiecki, *Bezpieczeństwo systemów…dz. cyt.*, s. 26-27.

Rysunek 3.5. Planuj-wykonuj-sprawdzaj-działaj (PDCA), wykorzystywany w procesach systemu zarządzania bezpieczeństwem informacji (SZBI)



Źródło: Opracowanie własne na podstawie, F. Wołowski, J. Zawiła-Niedźwiecki, *Bezpieczeństwo systemów informacyjnych. Praktyczny przewodnik zgodny z normami polskimi i międzynarodowymi*, Wydawnictwo edu-Libri, Kraków-Warszawa 2012, s. 28.

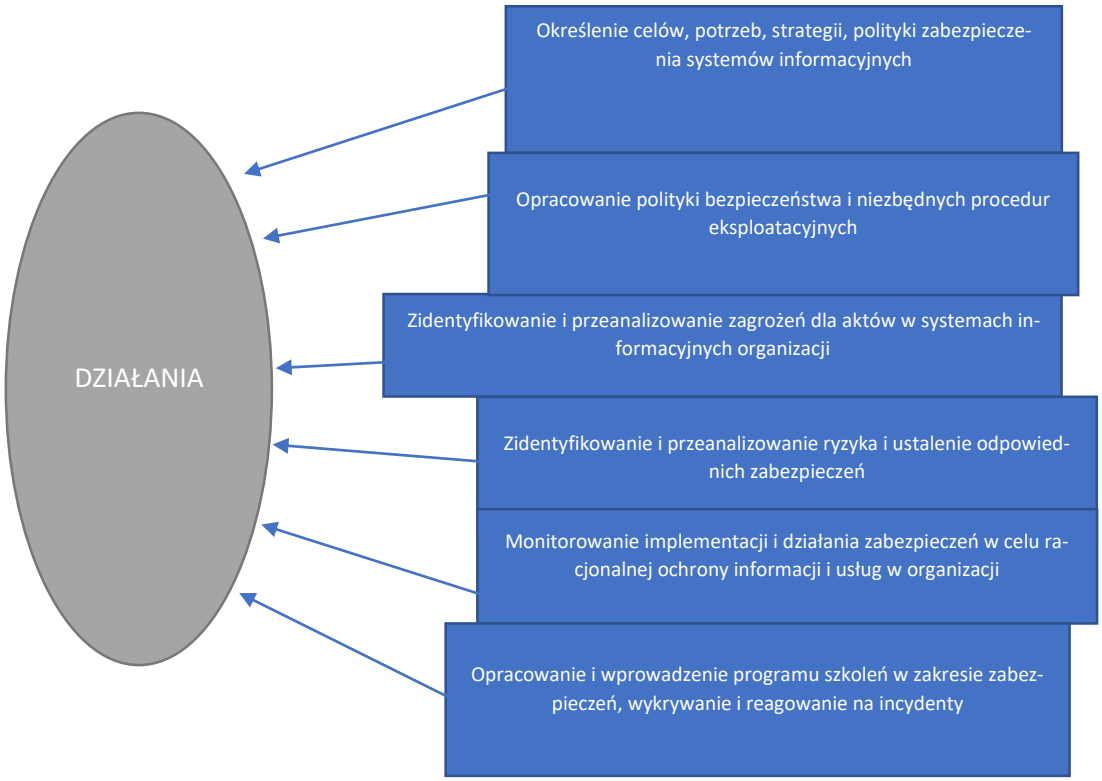
Pierwszy etap cyklu *ustanowienia* SZBI wymaga ustalenia zakresu działania jak i polityki w obszarze doskonalenia bezpieczeństwa informacji z zachowaniem spójności z prawnymi aspektami oraz przyjętymi celami organizacji. Drugi etap *wdrożenia i eksploatacji* dotyczy implementacji procedur, środków zaradczych związanych z zarządzaniem ryzykiem, zabezpieczeń zdolnych do szybkiego wykrywania incydentów naruszających bezpieczeństwo informacji czy szkoleń pracowników. W trzecim etapie, jakim jest *monitorowanie i przegląd* dokonuje się weryfikacji stopnia efektywności SZBI, weryfikacji błędów systemowych, przeglądów SZBI przez kierownictwo i audytów wewnętrznych. Etap końcowy *utrzymanie i doskonalenie* wykonuje się działania korygujące, które są reakcją na wykryte błędy lub prewencyjne[1].

Zarządzanie bezpieczeństwem informacyjnym to proces prowadzony w celu osiągnięcia i utrzymywania odpowiedniego poziomu poufności, integralności, dostępności,

[1] M. Majchrzak, *Zarządzanie bezpieczeństwem informacyjnym*, [w:] Prakseologia w zarządzaniu i dowodzeniu. Racjonalność w zarządzaniu. Część 2, red. W. Kieżun, J. Wołejszo, A. Pisarska, Kaliskie Towarzystwo Przyjaciół Nauk, Kalisz 2020, s. 113.

rozliczalności, autentyczności i niezawodności informacji. Na rysunku 3.6 zostały przedstawione najistotniejsze działania w zarządzaniu bezpieczeństwa systemów informacyjnych.

Rysunek 3.6. Działania w zarzadzaniu bezpieczeństwem systemów informacyjnych



Źródło: Opracowanie własne na podstawie F. Wołowski, J. Zawiła-Niedźwiecki, *Bezpieczeństwo systemów informacyjnych. Praktyczny przewodnik zgodny z normami polskimi i międzynarodowymi*, Wydawnictwo edu-Libri, Kraków-Warszawa 2012, *s. 23-24.*

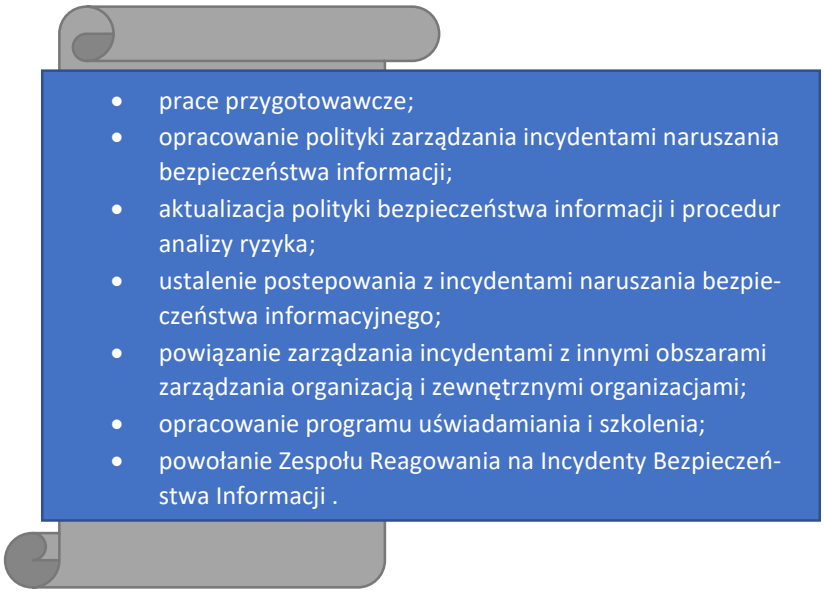
Efektywność wymienionych działań wymaga spójności ze strategią rozwoju organizacji oraz propagowania kultury bezpieczeństwa informacyjnego wśród uczestników tych procesów ze wskazaniem uzyskanych wyników, wdrożonych prac i podejmowanych decyzji. Zarządzanie bezpieczeństwem informacyjnym jest ściśle powiązane z polityką bezpieczeństwa, która powinna uwzględniać wymagania normy ISO/IEC 27001:2005 dotyczące zarządzania bezpieczeństwem informacyjnym w organizacjach w kontekście specyfiki ich działalności.

Politykę bezpieczeństwa można podzielić na obszary, które się wzajemnie uzupełniają oraz przenikają a są nimi:

- politykę ochrony technicznej, związaną z ochroną mienia personelu danej społeczności, pomieszczeń, budynków, organizacji zawierającej różnego rodzaju instrukcje zabezpieczeń, procedury na wypadek incydentów bezpieczeństwa lub sytuacji zagrożeń;
- politykę personalną, mającą ścisły związek z odpowiednim doborem personelu na dane stanowiska, procedurami dotyczącymi zapoznania pracowników z zadaniami bezpieczeństwa, szkoleniem pracowników oraz wprowadzeniem odpowiednich procedur działań na wypadek braku odpowiedniego personelu;
- politykę bezpieczeństwa informacji, związaną z zarządzaniem i ochroną informacji stanowiących tajemnicę społeczności i informacji prawnie chronionych;
- politykę organizacyjną, zawierającą procedury organizacyjne, w tym procedury utrzymania ciągłości działania, plany awaryjne na wypadek katastrofy, związane z zapasowymi ośrodkami przetwarzania[1].

Według badaczy bezpieczeństwa informacyjnego F. Wołowskiego i J. Zawiły Niedźwieckiego od dokładności przeprowadzenia weryfikacji incydentu zależy, jakość realizowanych w przyszłości prac związanych z zarządzaniem incydentami.

Rysunek 3.7. Czynności w strategii zarządzania incydentami



Źródło: Opracowanie własne na podstawie F. Wołowski, J. Zawiła-Niedźwiecki, *Bezpieczeństwo systemów informacyjnych. Praktyczny przewodnik zgodny z normami polskimi i międzynarodowymi*, Wydawnictwo edu-Libri, Kraków-Warszawa 2012, s. 142-153.

[1] J. Janczak, A. Nowak, *Bezpieczeństwo informacyjne…dz. cyt.*, s. 80-81.

Uczeni zgodnie zajmują stanowisko, że po jego zakończeniu organizacja powinna być w pełni przygotowana do właściwego zarządzania incydentami. Rysunek 3.7 wskazuje czynności w strategii zarządzania incydentami. Powyższe działania wpływają na skuteczność i efektywność w zachowaniu bezpieczeństwa informacji. Wymagają jednakże ustawicznej kontroli oraz podnoszenia świadomości zagrożeń, jakie mogą dotknąć użytkowników systemów informacyjnych.

3.3. Standardy i normy bezpieczeństwa systemu informacyjnego w uczelni wyższej

Szczególne wyzwania jak i zagrożenia bezpieczeństwa systemów informacyjnych wynikające z procesów globalizacyjnych są przedmiotem badań. Władze uczelni wyższej, czyli rektor kieruje jednostką sektora publicznego, ponosi też pełną odpowiedzialność nie tylko za sprawy finansowe, które zgodnie z literą prawa wymagają kontroli alokacji zasobów. Jest także odpowiedzialny za zapewnienie bezpieczeństwa systemów informacyjnych wykorzystywanych w organizacji tj. przekazywania, komunikacji między pracownikami oraz interesariuszami zewnętrznymi[1]. Doskonałym narzędziem w celu weryfikacji aktualnego stanu zagrożeń, ograniczeń bezpieczeństwa systemu informacyjnego w uczelni wyższej jest audyt wewnętrzny. Jest to działalność niezależna, obiektywna, a jej celem jest przysporzenie wartości i usprawnienie działalności operacyjnej organizacji. Polega na systematycznej i dokonywanej w uporządkowany sposób ocenie procesów zarządzania ryzykiem, kontroli, ładu organizacyjnego i przyczynia się do poprawy działania[2]. Organizacja pojmowana jest, jako system złożony z ludzi, technicznych środków działania i sposobów[3].

Wewnętrzny mechanizm kierowania organizacją to *internal control*, czyli ogół działań podejmowanych dla zapewnienia realizacji celów jak i zadań w sposób zgodny z prawem. Mający miano efektywnego, oszczędnego, terminowego. Dokonywana przez władzę uczelni weryfikacja obecnego stanu bezpieczeństwa systemów informacyjnych służy, jako zapewnienie:

- ochrony zasobów informacyjnych i wiarygodności użytkowników;

[1] M. Majchrzak, *Sposoby przeprowadzania samooceny oraz prezentacja i wykorzystanie jej wyników w procesie zarządzania jednostką organizacyjną*, „Studia Kaliskie", t. 6, 2018, s.184-185.
[2] A. Sekuła, *Kryteria oceny ustaleń stanu faktycznego w audycie wewnętrznym*, Wydawnictwo Polskiego Instytutu Kontroli Wewnętrznej., Warszawa 2015, s. 9.
[3] J. Wołejszo, *Prakseologia w zarządzaniu i dowodzeniu*, „Studia Kaliskie", t. 2, 2014, s. 30.

- skuteczności i efektywności działania systemu informacyjnego w uczelni wyższej;
- zgodności działalności z przepisami prawa oraz unormowaniami wewnętrznymi;
- reagowania na incydenty i identyfikacji zagrożeń bezpieczeństwa systemu informacyjnego;
- zarządzanie ryzykiem w obszarze informacji i efektywność oraz skuteczność przepływu informacji[1].

Dokumentem zawierającym zestaw praw, reguł, praktycznych doświadczeń dotyczących sposobu zarządzania, ochrony i dystrybucji danych osobowych wewnątrz uczelni wyższej jest *Polityka bezpieczeństwa.* Dokument ten odnosi się do zabezpieczenia danych osobowych w uczelni wyższej, zarówno do zabezpieczenia danych przetwarzanych tradycyjnie, jak i danych przetwarzanych w systemach informatycznych. Wskazuje działania, jakie należy wykonać oraz ustanawia zasady, reguły postępowania, które trzeba należycie stosować we właściwy sposób zabezpieczyć dane osobowe. Ma także na celu osiągnięcie takiego poziomu organizacyjnego i technicznego systemu zarządzania bezpieczeństwem informacji. Polityka bezpieczeństwa ma zastosowanie do wszystkich jednostek znajdujących się w uczelni wyższej a obowiązkiem pracowników jest przestrzeganie postanowień w niej zapisanych.

Taka polityka ma zapewnić w uczelni wyższej następujące reguły, jakimi są:

- poufności, czyli zapewnienie dostępu do informacji wyłącznie takim podmiotom, które są do tego upoważnione;
- integralności czyli zapewnienie dokładności i kompletności danych i informacji jak również w pewien sposób określenie metod ich przetwarzania;
- dostępności informacji, czyli zapewnienie, iż osoby upoważnione mają dostęp do informacji oraz związanych z nią aktywów tylko w przypadku, gdy zachodzi taka potrzeba;
- rozliczalności, czyli zapewnienie przechowywania pełnej historii dostępu do danych wraz z informacją o osobie, która taki dostęp posiada lub posiadała i w jakim zakresie[2].

Zasady i standardy określone w dokumentacji powinny być stosowane przez wszystkich pracowników uczelni wyższej, w związku z powyższym każdy pracownik jest zobligowany do zapoznania się z dokumentacją i do bezwzględnego przestrzegania

[1] Ustawa z dnia 27 sierpnia 2009 *o finansach publicznych*, Dz. U. z 2009, Nr 157, poz. 1240, art. 68.
[2] https://monitor.uksw.edu.pl/docs/download/2939287b3c61177a675bd574eeb16494, [dostęp:28.12.2023].

zasad w niej zawartych. Każdy pracownik, powinien być pełen świadomej odpowiedzialności, jak ma postępować zgodnie z przyjętymi zasadami i minimalizować zagrożenia wynikające z błędów ludzkich. W przypadku naruszenia bezpieczeństwa informacji stosuje się procedury postępowania stworzone dla takiej sytuacji, a pracownicy ponoszą odpowiedzialność dyscyplinarną i prawną wynikającą z przepisów prawa, Kodeksu Cywilnego oraz Kodeksu Pracy.

Administrator Danych Osobowych (ADO) zobowiązany jest do zapewnienia zgodności przetwarzania danych osobowych z przepisami prawa, ochrony przetwarzania danych osobowych przed ich udostępnieniem osobom nieupoważnionym. Ponadto ADO zobowiązany jest zapewnić kontrolę i rozliczalność nad tym, jakie dane osobowe, kiedy i przez kogo są przetwarzane oraz komu są przekazywane. W tym celu ADO prowadzi dokumentację oraz wszelkie potrzebne ewidencje i upoważnienia.

W dokumencie dotyczącym polityki bezpieczeństwa informacji oraz danych przechowywanych jak i przetwarzanych w uczelni wyższej szczególną uwagę zwraca się na dostęp i zabezpieczenia, czyli:

- wydzielenie obszarów przeznaczonych do przetwarzania oraz przechowywania danych od obszarów dostępnych na ogólną skalę jak i zapewnienie odpowiednich barier fizycznych mających przeciwdziałać dostępowi nieuprawnionemu;
- zarządzaniu uprawnieniami poszczególnych użytkowników z zastosowaniem zasady związanej minimalizacją uprawnień;
- stosowanie zasady dostępu ograniczonego;
- stosowanie zabezpieczeń systemów przetwarzania informacji, wielowarstwowych;
- monitorowanie dogłębne i adekwatne skuteczności stosowanych w uczelni wyższej środków kontroli dostępu do informacji w ramach audytów wewnętrznych.

Struktury zbiorów i przepływu danych między systemami na uczelni wyższej działają przy zastosowaniu systemów informacyjnych. Zbiory zlokalizowane są w bazach danych, umieszczonych na serwerach bazodanowych i przetwarzane w dostosowanych do tego programach. Zawartość pól informacyjnych w programach powinna być zgodna z literą prawa w zakresie przetwarzania danych osobowych. Przepływ informacji pomiędzy systemami może dokonywać się dwukierunkowo bądź jednokierunkowo.

Przesyłanie danych może odbywać się w sposób:

- manualny, wykorzystując nośniki zewnętrzne;

- półautomatyczny, wykorzystując funkcję eksportu/importu danych za pomocą teletransmisji za pośrednictwem wewnętrznej sieci teleinformatycznych;
- automatyzowany m.in. ERP-> USOS, USOS->LDAP.

Przesyłanie danych za pomocą poczty elektronicznej jest dopuszczalne tylko w przypadku, gdy nadawca i adresat mają ważne upoważnienia do przetwarzania danych osobowych oraz gdy do przesyłania wiadomości wykorzystywane są konta w domenie uczelnianej a w razie przesyłania informacji wrażliwych z danymi osobowymi pliki przesyłane powinny być koniecznie kodowane (zabezpieczone hasłem).

Odnosząc się do polityki zarzadzania kopiami zapasowymi należy pamiętać, iż:

- każde istotne dane są archiwizowane na wypadek awarii;
- wszelkie posiadane nośniki z kopiami zapasowymi powinny być przechowywane w takim miejscu, do którego nie mają dostępu osoby trzecie i okresowo są one testowane;
- za wszelkiego rodzaju tworzone kopie odpowiada powołany przez władze pracownik z IT, może wykonać to również inna osoba tzw. operator w przypadku nieobecności pracownika odpowiedzialnego, a operatora wyznacza bezpośredni przełożony administratora;
- osoby upoważnione jedynie mają dostęp do sprzętu umieszczonego w serwerowni oraz nośników, kopii zapasowych;
- wykorzystane nośniki kopii zapasowych są niszczone w sposób uniemożliwiający odtworzenie znajdujących się na nich danych[1].

W uczelni wyższej oprócz podstawowego dokumentu dotyczącego bezpieczeństwa informacji, jakim jest *polityka bezpieczeństwa informacji*, często zarządzeniem rektora wprowadza się wewnętrzne odrębnie dokumenty dotyczące bezpieczeństwa informacji. Z zakresu bezpieczeństwa informacji mogą to być dokumenty tj.: Instrukcja Zarządzania Systemami Informatycznymi Służącymi do Przetwarzania Danych Osobowych, Regulamin Zarządzania Incydentami Bezpieczeństwa Informacji, Regulamin Serwisu Internetowego, Regulamin korzystania ze służbowej poczty elektronicznej, Regulamin usługi zdalnego bezpiecznego dostępu do sieci uczelni (VPN), Instrukcja użytkowania komputerów w uczelni.

[1] https://monitor.uksw.edu.pl/docs/download/2939287b3c61177a675bd574eeb16494, [dostęp:28.12.2023].

W ramach świadczonych usług informacyjnych i pozostałych, uczelnia gromadzi informacje dotyczące urządzenia użytkownika, z którego nastąpiło połączenie a celem takiego działania będzie zapewnienie poprawności działania usług, adres IP komputera, informacje zawarte w plikach cookies lub innych technologiach. Uwzględnić należy dane dotyczące sesji, przeglądarki internetowej, aktywności na stronie i statystyk. Dane użytkowników pozwalają na poprawienie funkcjonowania serwisu internetowego oraz podniesieniu, jakości świadczonych usług jak również realizacji informacyjno-promocyjnych celów[1].

3.4. Charakterystyka zagrożeń i ograniczeń bezpieczeństwa systemu informacyjnego w uczelni wyższej

W uczelni wyższej jest powołany Inspektor Ochrony Danych, który czuwa nad realizacją podstawowych przepisów i zasad dotyczących ochrony osób fizycznych w związku z przetwarzaniem ich danych osobowych. Przepisy i zasady nie mogą, niezależnie od obywatelstwa czy miejsca zamieszkania naruszać podstawowych praw i wolności. Przetwarzanie danych osobowych powinno być zorganizowane w taki sposób, aby służyło społeczeństwu. Powyższe prawo nie jest prawem bezwzględnym, jednakże należy je postrzegać w kontekście jego społecznej funkcji a przede wszystkim wyważyć
w taki sposób względem innych praw podstawowych w myśl zasady proporcjonalności. Szybki postęp techniczny i globalizacja przyniosły kolejne wyzwania właśnie w dziedzinie ochrony danych osobowych. Wzrosła znacząco skala zbierania i wymiany danych osobowych. W związku z powyższym dzięki technologii, przedsiębiorstwa prywatne i organy publiczne mogą wykorzystywać dane osobowe w swojej działalności.

Wszelkie przemiany wymagają stabilnych ram ochrony danych w Unii oraz zdecydowanego ich egzekwowania, ponieważ bardzo ważna jest budowa zaufania, dzięki któremu będzie można zaobserwować rozwój gospodarki cyfrowej na rynku wewnętrznym[2]. Uczelnia posiada Klauzule RODO, czyli obowiązek informacyjny o przetwarzaniu danych osobowych. Zawarte są w niej informacje dotyczące tj.:

[1] https://www.uken.krakow.pl/polityka-prywatnosci, [dostęp: 5.12.2024].
[2] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. *w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych),* (Dz. Urz. UEL119 z 04.05.2016 r., str.1, z późn. zm.).

- administratora danych osobowych, jaka organizacja te dane będzie przetwarzała;
- wyznaczenie osoby na Inspektora Ochrony Danych Osobowych oraz w jaki sposób można się z nim skontaktować;
- w jakim celu odbywa się realizacja zadań ustawowych i statutowych i co należy do zakresu działania uczelni;
- komu uczelnia udostępnia dane osobowe na podstawie przepisów obowiązującego prawa czy zawartych umów;
- wskazany jest okres przetwarzania danych osobowych, możliwość wglądu do treści swoich danych w celu sprostowania pojawiających się nieprawidłowości[1].

Bardzo ważnym jest fakt dotyczący sposobu zabezpieczania systemu informatycznego przed złośliwym oprogramowaniem. Na każdym komputerze, na którym dochodzi do działań związanych z przetwarzaniem danych osobowych powinno być zgodnie z literą prawa zainstalowane oprogramowanie mające chronić komputer przed programem antywirusowym. Użytkownik komputera odpowiada za program antywirusowy wgrany na komputer.

Niedozwolone jest blokowanie, włączanie, odinstalowanie przez użytkowników oprogramowania zabezpieczającego komputer a w przypadku stwierdzenia na komputerze złośliwego oprogramowania użytkownik zobowiązany jest do zaprzestania wykonywania czynności i bezzwłoczne powiadomienie jednostki, która jest za informatyzację odpowiedzialna[2].

W badaniach empirycznych ocenie poddano jak użytkownicy oceniają zagrożenia systemu informacyjnego w uczelni wyższej. Za pomocą sondażu diagnostycznego w ramach oceny poglądu na temat zagrożeń systemu informacyjnego w uczelni wyższej przez respondentów takich grup jak: nauczyciele akademiccy, kadra administracyjna, studenci (różne roczniki), ankietowani mieli możliwość udzielenia jednej z pięciu zaproponowanych odpowiedzi:

13. Jak Państwo oceniają zagrożenia systemu informacyjnego w uczelni wyższej?

a) Klęski żywiołowe, pożar

Rozkład odpowiedzi respondentów grupy nauczyciele akademiccy i grupy kadra administracyjna dotyczący oceny przez użytkowników stopnia zagrożenia systemu uczelni wyższej przez klęski żywiołowe, pożar, prezentuje tabela 3.1.

[1] https://www.uken.krakow.pl/klauzula-rodo, [dostęp: 5.01.2024].
[2] https://www.uken.krakow.pl/klauzula-rodo, [dostęp: 5.01.2024].

Tabela 3.1. Odpowiedzi respondentów pracowników grupy nauczyciele akademiccy i grupy kadra administracyjna na temat zagrożeń systemu informacyjnego w szkole przez klęski żywiołowe, pożar

Odpowiedzi badanych osób: klęski żywiołowe, pożar						
Osoby poddane badaniu	**Respondenci nauczyciele akademiccy**		**Respondenci kadra administracyjna**		**OGÓŁEM**	
Ocena	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***
bardzo niska	345	69%	328	65,6%	673	67,3%
niska	85	17%	89	17,8%	174	17,4%
przeciętna	35	7%	36	7,2%	71	7,1%
wysoka	28	5,6%	21	4,2%	49	4,9%
bardzo wysoka	7	1,4%	26	5,2%	33	3,3%
	500	**100%**	**500**	**100%**	**1000**	**100%**

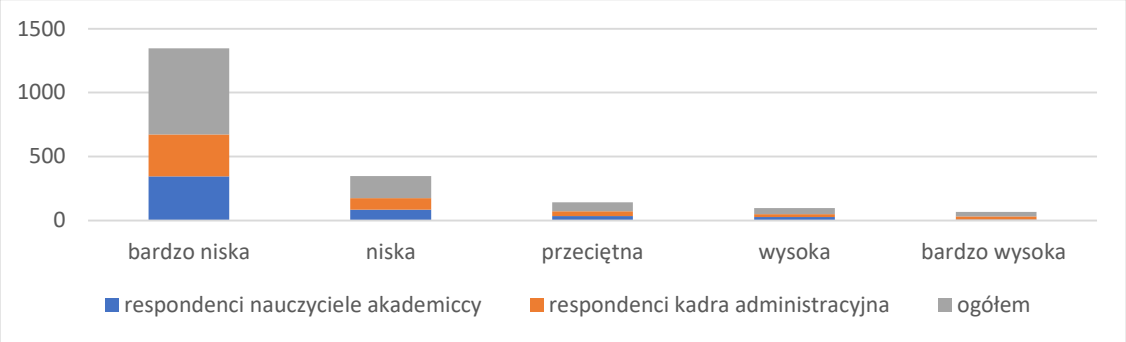
Źródło: opracowanie własne na podstawie badań własnych

Ogółem odpowiedzi na pytanie 13, podpunkt a) kwestionariusza ankiety dotyczącego oceny przez użytkowników stopnia zagrożenia systemu uczelni wyższej przez klęski żywiołowe, pożar. Odpowiedzi na to pytanie udzieliło 100%, respondentów z grupy nauczyciele akademiccy, kadra administracyjna, studenci (różne kierunki). W badaniu wzięło udział 500 osób zatrudnionych na stanowisku, nauczycieli akademickich oraz 500 osób zatrudnionych na stanowisku kadry administracyjnej.

Z przeprowadzonej analizy wynika, że nauczyciele akademiccy jak i kadra administracyjna ocenili stopień zagrożenia systemu uczelni wyższej przez klęski żywiołowe, pożar, jako bardzo niski. Wskazuje na to 345 respondentów, co w udziale procentowym wynosi 69% dla nauczycieli akademickich i 328 respondentów, co w udziale procentowym dla kadry administracyjnej wynosi 65%. Analizując udzielone odpowiedzi w opinii 7 respondentów, co w udziale procentowym wynosi 1,4% dla nauczycieli akademickich i 26 respondentów, co w udziale procentowym daje 5,2% dla kadry administracyjnej świadczy ze pojawienie się klęski żywiołowej stanowi bardzo duże zagrożenie dla systemu informacyjnego uczelni wyższej.

Wykres 3.1. przedstawia odpowiedzi respondentów grupy nauczyciele akademiccy i grupy kadry administracyjnej na temat stopnia zagrożenia systemu uczelni wyższej przez klęski żywiołowe, pożar.

Wykres 3.1. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy kadra naukowa na temat stopnia zagrożenia systemu uczelni wyższej przez klęski żywiołowe, pożar



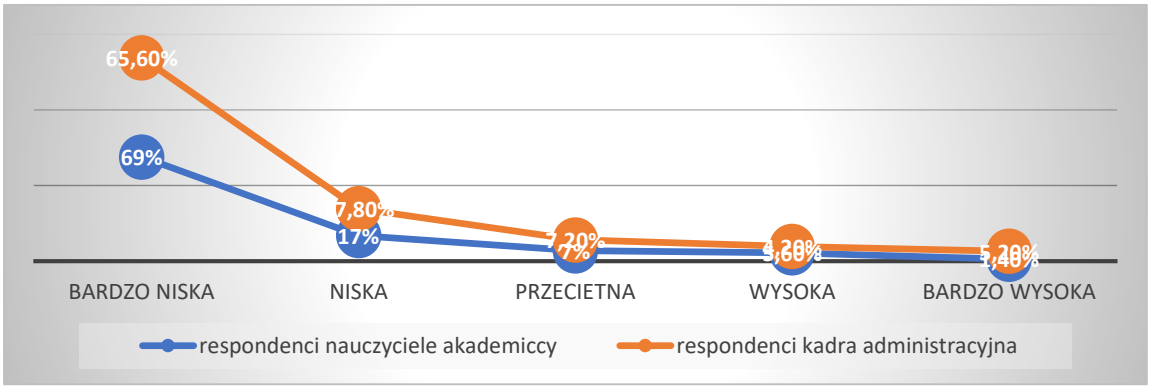
Źródło: opracowanie własne na podstawie badań własnych

O stopniu zależności świadczy współczynnik korelacji liniowej Pearsona na poziomie 0,99 i współczynnik determinacji liniowej, który wskazuje procent wyjaśnionej liniowo zmienności równy 98,01%. Wykres 3.2. pokazuje zależność między respondentami grupy nauczyciele akademiccy i grupy kadra administracyjna pod względem stopnia zagrożenia systemu uczelni wyższej przez klęski żywiołowe oraz pożar.

$$r_{xy} = \frac{\frac{1}{n}\sum_{i=1}^{n}(x_i-\bar{x})(y_i-\bar{y})}{S_x S_y}=0{,}99$$

$$\text{WD}=r\frac{2}{xy} * 100\% = 98{,}01\%$$

Wykres 3.2. Zależność między respondentami grupy nauczyciele akademiccy i grupy kadra administracyjna pod względem stopnia zagrożenia systemu uczelni wyższej przez klęski żywiołowe, pożar



Źródło: opracowanie własne na podstawie badań własnych

W związku z faktem, że wartość liczbowa w ocenie relacji jest dodatnia oznacza to, iż wraz ze wzrostem wartości jednej zmiennej rosną wartości także drugiej. Tabela

3.2. przedstawia odpowiedzi respondentów grupy nauczyciele akademiccy i grupy studenci (różne kierunki) na temat zagrożeń systemu informacyjnego w uczelni wyższej przez klęski żywiołowe, pożar.

Tabela. 3.2. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupa studenci (różne kierunki) na temat zagrożeń systemu informacyjnego w uczelni wyższej przez klęski żywiołowe, pożar

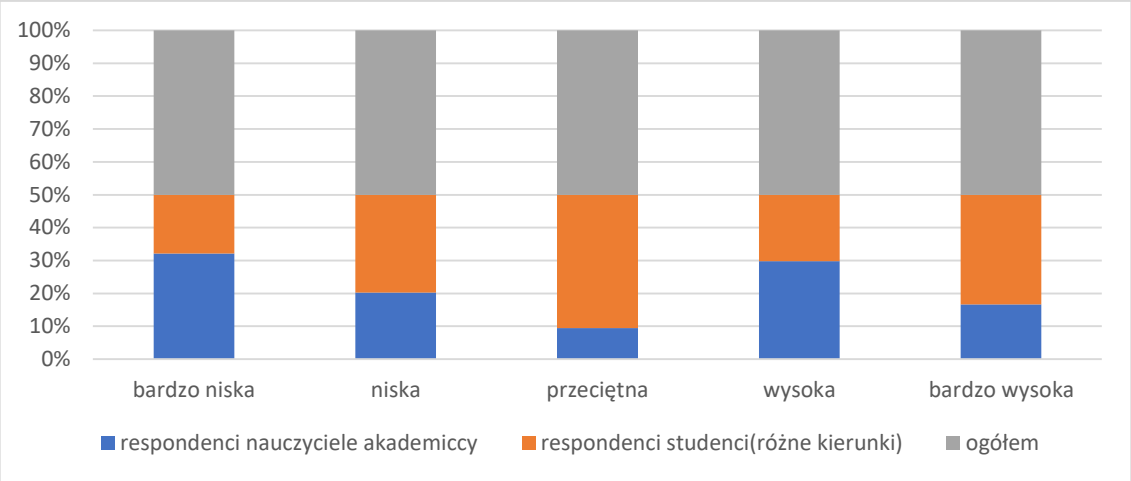
Odpowiedzi badanych osób klęski żywiołowe, pożar						
Osoby poddane badaniu	**Respondenci nauczyciele akademiccy**		**Respondenci studenci (różne kierunki)**		**OGÓŁEM**	
Ocena	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***
bardzo niska	345	69%	192	38,4%	537	53,7%
niska	85	17%	125	25%	210	21%
przeciętna	35	7%	150	30%	185	18,5%
wysoka	28	5,6%	19	3,8%	47	4,7%
bardzo wysoka	7	1,4%	14	2,8%	21	2,1%
	500	**100%**	**500**	**100%**	**1000**	**100%**

Źródło: opracowanie własne na podstawie badań własnych

W badaniu wzięło udział 500 osób zatrudnionych na stanowisku, nauczycieli akademickich oraz 500 osób studiujących w uczelni wyższej. Z przeprowadzonej analizy wynika, że nauczyciele akademiccy jak i studenci (różne kierunki) ocenili stopień zagrożenia systemu uczelni wyższej przez klęski żywiołowe, pożar jako bardzo niski. Wskazuje na to 345 respondentów, co w udziale procentowym wynosi 69% dla nauczycieli akademickich i 192 respondentów, co w udziale procentowym dla studentów (różne roczniki) wynosi 38,4%.

Analizując udzielone odpowiedzi w opinii 7 respondentów, co w udziale procentowym wynosi 1,4% dla nauczycieli akademickich i 14 respondentów, co w udziale procentowym daje 2,8% dla studentów studiujących w uczelni wyższej świadczy, że pojawienie się klęski żywiołowej stanowi bardzo duże zagrożenie dla systemu informacyjnego uczelni wyższej. Wykres 3.3. przedstawia odpowiedzi respondentów grupy nauczyciele akademiccy i grupy studenci (różne kierunki) na temat stopnia zagrożenia systemu uczelni wyższej przez klęski żywiołowe, pożar.

Wykres 3.3. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy studenci (różne kierunki) na temat stopnia zagrożenia systemu uczelni wyższej przez klęski żywiołowe, pożar



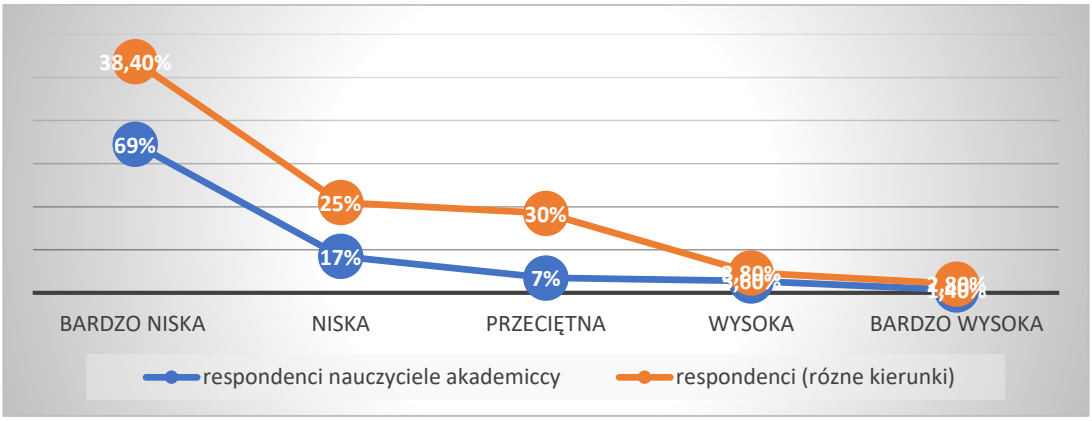
Źródło: opracowanie własne na podstawie badań własnych

O stopniu zależności świadczy współczynnik korelacji liniowej Pearsona na poziomie 0,73 i współczynnik determinacji liniowej, który wskazuje procent wyjaśnionej liniowo zmienności równy 53,29%. Wykres 3.4. pokazuje zależność między respondentami grupy nauczyciele akademiccy i grupy studenci (różne kierunki) pod względem stopnia zagrożenia systemu uczelni wyższej przez klęski żywiołowe, pożar.

$$r_{xy} = \frac{\frac{1}{n}\sum_{i=1}^{n}(x_i-\bar{x})(y_i-\bar{y})}{S_x S_y}=0{,}73$$

$$\text{WD}=r_{xy}^{2} * 100\% = 53{,}29\%$$

Wykres 3.4. Zależność między respondentami grupy nauczyciele akademiccy i grupy studenci (różne kierunki) pod względem stopnia zagrożenia systemu uczelni wyższej przez klęski żywiołowe, pożar



Źródło: opracowanie własne na podstawie badań własnych

W związku z faktem, że wartość liczbowa w ocenie relacji jest dodatnia oznacza to, iż wraz ze wzrostem wartości jednej zmiennej rosną wartości także drugiej. Tabela 3.3. przedstawia odpowiedzi respondentów grupy kadra administracyjna i grupy studenci (różne kierunki) na temat zagrożeń systemu informacyjnego w uczelni wyższej przez klęski żywiołowe, pożar.

Tabela 3.3. Odpowiedzi respondentów pracowników grupy kadra administracyjna i grupa studenci (różne kierunki na temat zagrożeń systemu informacyjnego w uczelni wyższej przez klęski żywiołowe, pożar

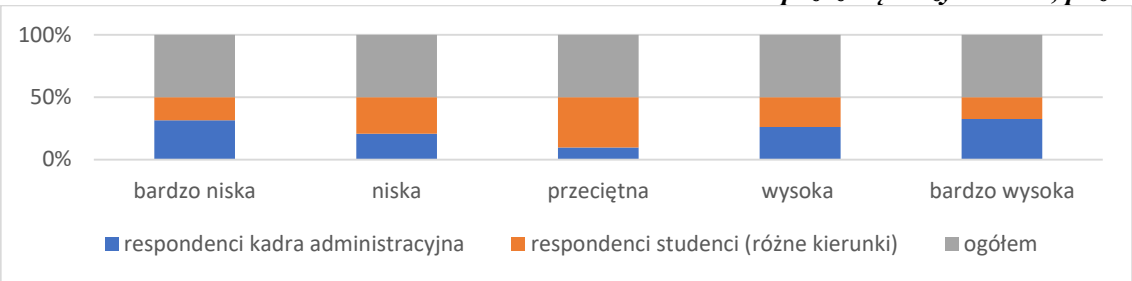
Odpowiedzi badanych osób klęski żywiołowe, pożar						
Osoby poddane badaniu	**Respondenci kadra administracyjna**		**Respondenci studenci (różne kierunki)**		**OGÓŁEM**	
Ocena	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***
bardzo niska	328	65,6%	192	38,4%	520	52%
niska	89	17,8%	125	25%	214	21,4%
przeciętna	36	7,2%	150	30%	186	18,6%
wysoka	21	4,2%	19	3,8%	40	4%
bardzo wysoka	26	5,2%	14	2,8%	40	4%
	500	**100%**	**500**	**100%**	**1000**	**100%**

Źródło: opracowanie własne na podstawie badań własnych

W badaniu wzięło udział 500 osób zatrudnionych na stanowisku, kadry administracyjnej oraz 500 osób studiujących w uczelni wyższej. Z przeprowadzonej analizy wynika, że kadra administracyjna, jak i studenci (różne kierunki) ocenili stopień zagrożenia systemu uczelni wyższej przez klęski żywiołowe, pożar, jako bardzo niski. Wskazuje na to 328 respondentów, co w udziale procentowym wynosi 65,6% dla kadry administracyjnej i 192 respondentów, co w udziale procentowym dla studentów (różne roczniki) wynosi 38,4%.

Analizując udzielone odpowiedzi w opinii 26 respondentów, co w udziale procentowym wynosi 5,2% dla kadry administracyjnej i 14 respondentów, co w udziale procentowym daje 2,8% dla studentów studiujących w uczelni wyższej świadczy, że pojawienie się klęski żywiołowej stanowi bardzo duże zagrożenie dla systemu informacyjnego uczelni wyższej. Wykres 3.5. przedstawia odpowiedzi respondentów grupy kadra administracyjna i grupy studenci (różne kierunki) na temat stopnia zagrożenia systemu uczelni wyższej przez klęski żywiołowe, pożar.

Wykres 3.5. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy studenci (różne kierunki) na temat stopnia zagrożenia systemu uczelni wyższej przez klęski żywiołowe, pożar



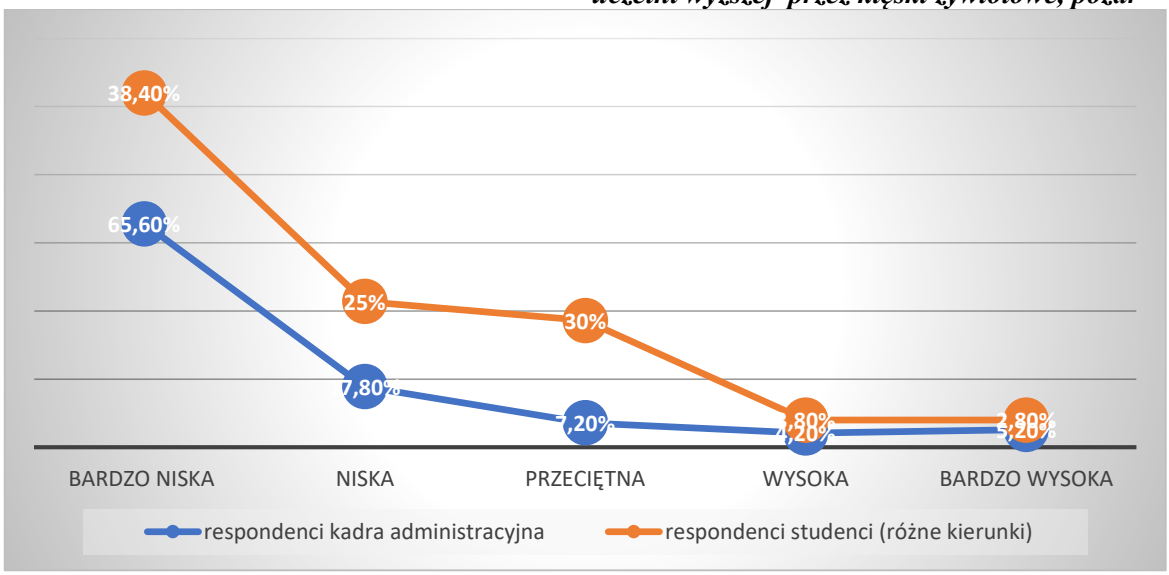
Źródło: opracowanie własne na podstawie badań własnych

O stopniu zależności świadczy współczynnik korelacji liniowej Pearsona na poziomie 0,73 i współczynnik determinacji liniowej, który wskazuje procent wyjaśnionej liniowo zmienności równy 53,29%. Wykres 3.6. pokazuje zależność między respondentami grupy kadra administracyjna i grupy studenci (różne kierunki) pod względem stopnia zagrożenia systemu uczelni wyższej przez klęski żywiołowe, pożar.

$$r_{xy} = \frac{\frac{1}{n}\sum_{i=1}^{n}(x_i-\bar{x})(y_i-\bar{y})}{s_x s_y}=0{,}73$$

$$\text{WD}=r_{xy}^{2} * 100\% = 53{,}29\%$$

Wykres 3.6. Zależność między respondentami grupy nauczyciele akademiccy i grupy studenci (różne kierunki) pod względem stopnia zagrożenia systemu uczelni wyższej przez klęski żywiołowe, pożar



Źródło: opracowanie własne na podstawie badań własnych

W związku z faktem, że wartość liczbowa w ocenie relacji jest dodatnia oznacza to, iż wraz ze wzrostem wartości jednej zmiennej rosną wartości także drugiej.

13. Jak Państwo oceniają zagrożenia systemu informacyjnego w uczelni wyższej?
b) Utrata danych

Rozkład odpowiedzi respondentów grupy nauczyciele akademiccy i kadra administracyjna dotyczących oceny przez użytkowników stopnia zagrożenia systemu uczelni wyższej przez utratę danych prezentuje tabela 3.4.

Tabela. 3.4. Odpowiedzi respondentów pracowników grupy nauczyciele akademiccy i grupa kadra administracyjna na temat zagrożeń systemu informacyjnego w uczelni wyższej przez utratę danych

Odpowiedzi badanych osób utrata danych						
Osoby poddane badaniu	**Respondenci nauczyciele akademiccy**		**Respondenci kadra administracyjna**		**OGÓŁEM**	
Ocena	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***
bardzo niska	35	7%	17	3,4%	52	5,2%
niska	26	5,2%	18	3,6%	44	4,4%
przeciętna	378	75,6%	96	19,2%	474	47,4%
wysoka	33	6,6%	82	16,4%	115	11,5%
bardzo wysoka	28	5,6%	287	57,4%	315	31,5%
	500	**100%**	**500**	**100%**	**1000**	**100%**

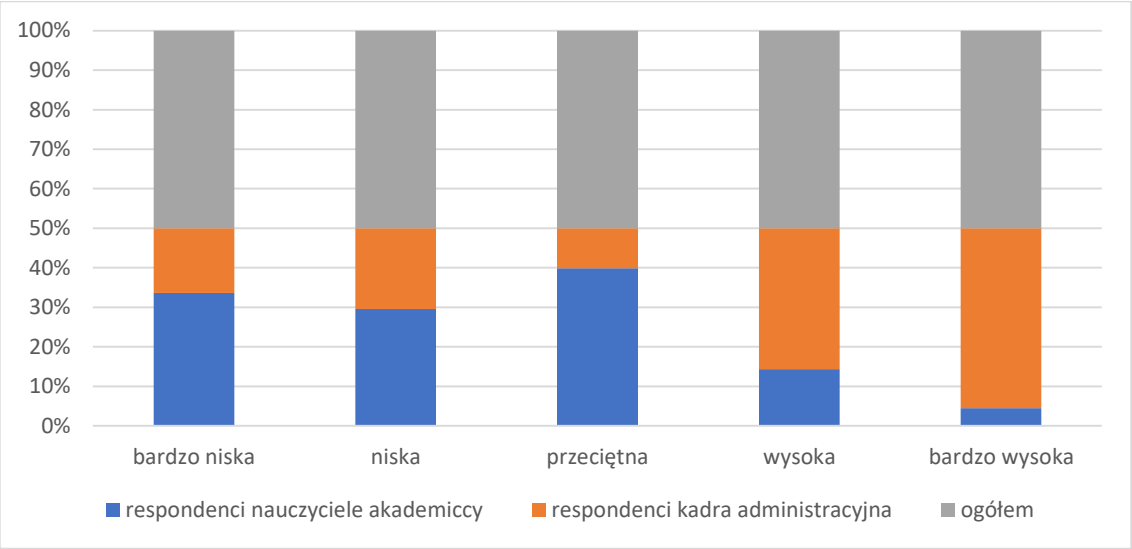
Źródło: opracowanie własne na podstawie badań własnych

W badaniu wzięło udział 500 osób zatrudnionych na stanowisku, nauczycieli akademickich oraz 500 osób zatrudnionych na stanowisku kadra administracyjna. Z przeprowadzonej analizy wynika, że nauczyciele akademiccy jak i kadra administracyjna ocenili stopień zagrożenia systemu uczelni wyższej przez utratę danych, jako przeciętną i bardzo wysoką. Wskazuje na to 378 respondentów, co w udziale procentowym wynosi 75,6% dla nauczycieli akademickich i 287 respondentów, co w udziale procentowym dla kadry administracyjnej wynosi 57,4%.

Analizując udzielone odpowiedzi w opinii 35 respondentów, co w udziale procentowym wynosi 7% dla nauczycieli akademickich i 17 respondentów, co w udziale procentowym daje 3,4% dla kadry administracyjnej świadczy, że pojawienie się utraty danych stanowi bardzo niskie zagrożenie dla systemu informacyjnego uczelni wyższej.

Wykres 3.7. przedstawia odpowiedzi respondentów grupy nauczyciele akademiccy i grupy kadra administracyjna na temat stopnia zagrożenia systemu uczelni wyższej przez utratę danych.

Wykres 3.7. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy kadra administracyjna na temat stopnia zagrożenia systemu uczelni wyższej przez utratę danych



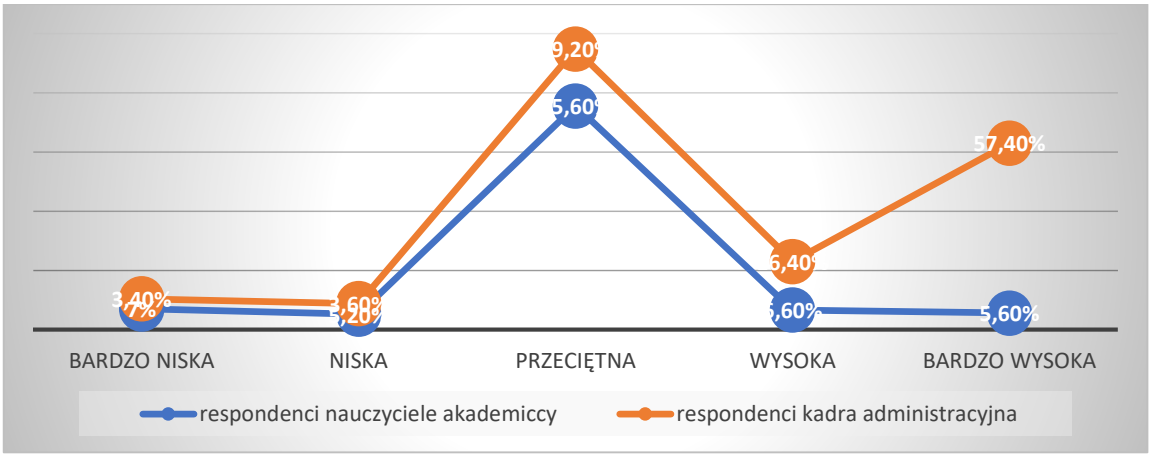
Źródło: opracowanie własne na podstawie badań własnych

O stopniu zależności świadczy współczynnik korelacji liniowej Pearsona na poziomie - 0,03 i współczynnik determinacji liniowej, który wskazuje procent wyjaśnionej liniowo zmienności równy 0,09%. Wykres 3.8. pokazuje zależność między respondentami grupy nauczyciele akademiccy i grupy kadra administracyjna pod względem stopnia zagrożenia systemu uczelni wyższej przez utratę danych.

$$r_{xy} = \frac{\frac{1}{n}\sum_{i=1}^{n}(x_i-\bar{x})(y_i-\bar{y})}{S_x S_y} = -0{,}03$$

$$WD = r_{xy}^2 * 100\% = 0{,}09\%$$

Wykres 3.8. Zależność między respondentami grupy nauczyciele akademiccy i grupy kadra administracyjna pod względem stopnia zagrożenia systemu uczelni wyższej przez utratę danych



Źródło: opracowanie własne na podstawie badań własnych

W związku z faktem, że wartość liczbowa w ocenie relacji jest ujemna oznacza to, iż wraz ze wzrostem wartości jednej zmiennej maleją wartości drugiej. Tabela 3.5. przedstawia odpowiedzi respondentów grupy nauczyciele akademiccy i grupy studenci (różne kierunki) na temat zagrożeń systemu informacyjnego w uczelni wyższej przez utratę danych.

Tabela 3.5. Odpowiedzi respondentów pracowników grupy nauczyciele akademiccy i grupy studentów (różne kierunki) na temat zagrożeń systemu informacyjnego w uczelni wyższej przez utratę danych

Odpowiedzi badanych osób utrata danych						
Osoby poddane badaniu	**Respondenci nauczyciele akademiccy**		**Respondenci studenci (różne kierunki)**		**OGÓŁEM**	
Ocena	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***
bardzo niska	35	7%	92	18,4%	127	12,7%
niska	26	5,2%	165	33%	191	19,1%
przeciętna	378	75,6%	178	35,6%	556	55,6%
wysoka	33	6,6%	36	7,2%	69	6,9%
bardzo wysoka	28	5,6%	29	5,8%	57	5,7%
	500	**100%**	**500**	**100%**	**1000**	**100%**

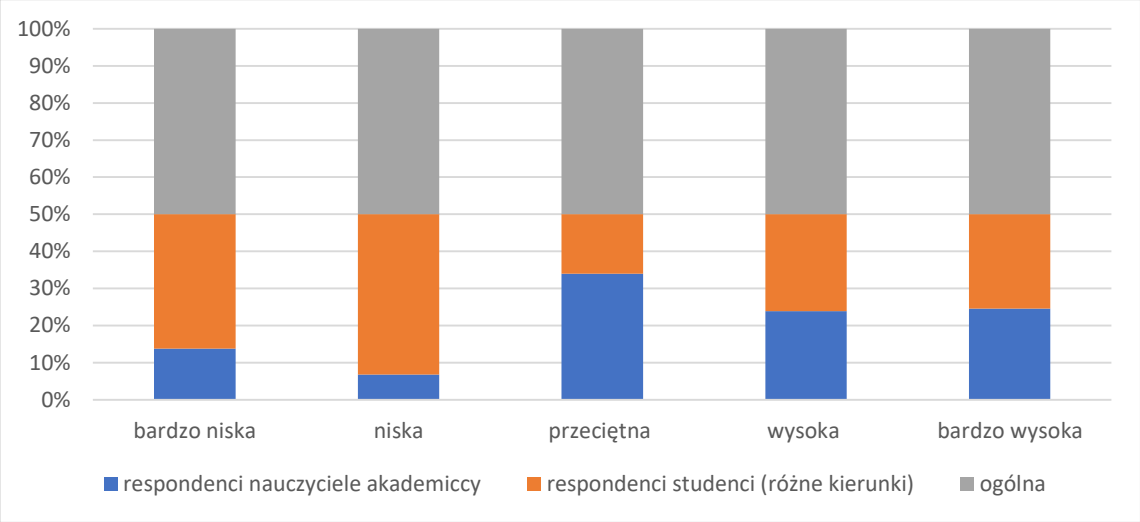
Źródło: opracowanie własne na podstawie badań własnych

W badaniu wzięło udział 500 osób zatrudnionych na stanowisku, nauczycieli akademickich oraz 500 osób studiujących w uczelni wyższej. Z przeprowadzonej analizy wynika, że nauczyciele akademiccy jak i studenci (różne kierunki) ocenili stopień zagrożenia systemu uczelni wyższej przez utratę danych jako przeciętny. Wskazuje na to 378 respondentów, co w udziale procentowym wynosi 75,6% dla nauczycieli akademickich i 178 respondentów, co w udziale procentowym dla studentów (różne roczniki) wynosi 35,6%.

Analizując udzielone odpowiedzi w opinii 28 respondentów, co w udziale procentowym wynosi 5,6% dla nauczycieli akademickich i 29 respondentów, co w udziale procentowym daje 5,8% dla studentów studiujących w uczelni wyższej świadczy, że pojawienie się utraty danych stanowi bardzo duże zagrożenie dla systemu informacyjnego uczelni wyższej.

Wykres 3.9. przedstawia odpowiedzi respondentów grupy nauczyciele akademiccy i grupy kadra administracyjna na temat stopnia zagrożenia systemu uczelni wyższej przez utratę danych.

Wykres 3.9. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy studenci (różne kierunki) na temat stopnia zagrożenia systemu uczelni wyższej przez utratę danych



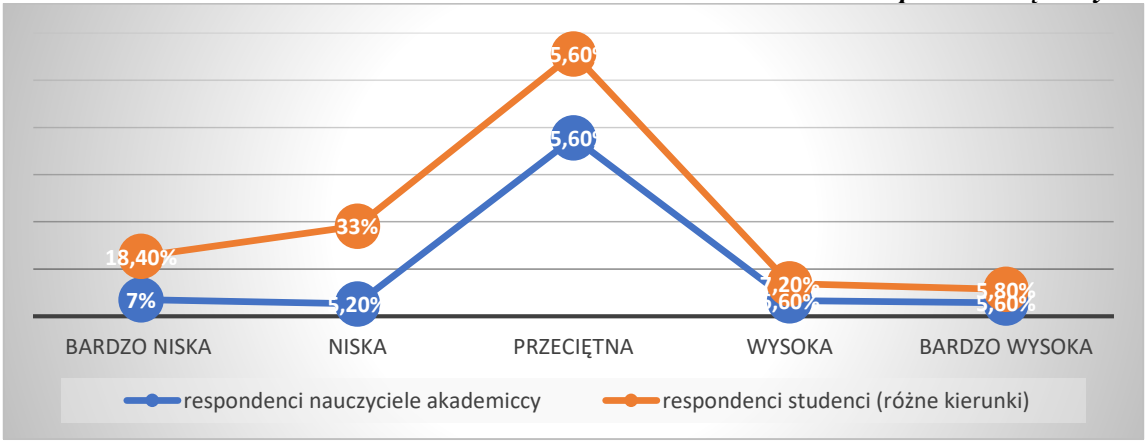
Źródło: opracowanie własne na podstawie badań własnych

O stopniu zależności świadczy współczynnik korelacji liniowej Pearsona na poziomie 0,62 i współczynnik determinacji liniowej, który wskazuje procent wyjaśnionej liniowo zmienności równy 38,44%. Wykres 3.10. pokazuje zależność między respondentami grupy nauczyciele akademiccy i grupy studenci (różne kierunki) pod względem stopnia zagrożenia systemu uczelni wyższej przez utratę danych.

$$r_{xy} = \frac{\frac{1}{n}\sum_{i=1}^{n}(x_i-\bar{x})(y_i-\bar{y})}{S_x S_y}=0{,}62$$

$$\text{WD}=r_{xy}^{2} * 100\% = 38{,}44\%$$

Wykres 3.10. Zależność między respondentami grupy nauczyciele akademiccy i grupy studenci (różne kierunki) pod względem stopnia zagrożenia systemu uczelni wyższej przez utratę danych



Źródło: opracowanie własne na podstawie badań własnych

W związku z faktem, że wartość liczbowa w ocenie relacji jest dodatnia oznacza to, iż wraz ze wzrostem wartości jednej zmiennej rosną wartości także drugiej. Tabela 3.6. przedstawia odpowiedzi respondentów grupy kadra administracyjna i grupy studenci (różne kierunki) na temat zagrożeń systemu informacyjnego w uczelni wyższej przez utratę danych.

Tabela 3.6. Odpowiedzi respondentów pracowników grupy kadra administracyjna i grupy studentów (różne kierunki) na temat zagrożeń systemu informacyjnego w uczelni wyższej przez utratę danych

Odpowiedzi badanych osób utrata danych						
Osoby poddane badaniu	**Respondenci kadra administracyjna**		**Respondenci studenci (różne kierunki)**		**OGÓŁEM**	
Ocena	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***
bardzo niska	17	3,4%	92	18,4%	109	10,9%
niska	18	3,6%	165	33%	183	18,3%
przeciętna	96	19,2%	178	35,6%	274	27,4%
wysoka	82	16,4%	36	7,2%	118	11,8%
bardzo wysoka	287	57,4%	29	5,8%	316	31,6%
	500	**100%**	**500**	**100%**	**1000**	**100%**

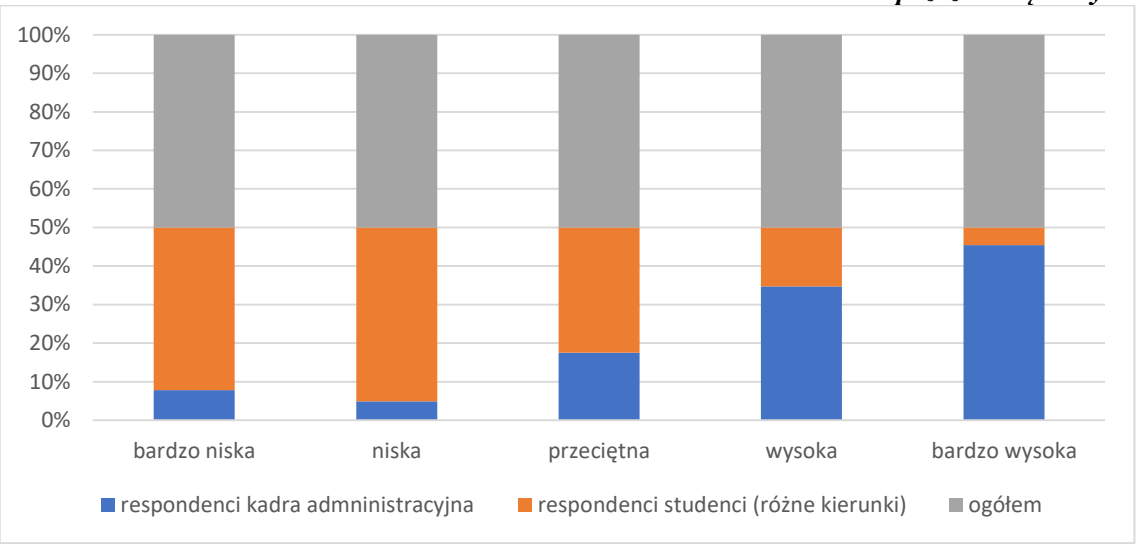
Źródło: opracowanie własne na podstawie badań własnych

W badaniu wzięło udział 500 osób zatrudnionych na stanowisku, kadry administracyjnej oraz 500 osób studiujących w uczelni wyższej. Z przeprowadzonej analizy wynika, że kadra administracyjna jak i studenci (różne kierunki) ocenili stopień zagrożenia systemu uczelni wyższej przez utratę danych jako bardzo wysoki i przeciętny. Wskazuje na to 287 respondentów, co w udziale procentowym wynosi 57,4% dla kadry administracyjnej i 178 respondentów, co w udziale procentowym dla studentów (różne roczniki) wynosi 35,6%.

Analizując udzielone odpowiedzi w opinii 17 respondentów, co w udziale procentowym wynosi 3,4% dla kadry administracyjnej i 92 respondentów, co w udziale procentowym daje 18,4% dla studentów studiujących w uczelni wyższej świadczy, że pojawienie się uraty danych stanowi bardzo małe zagrożenie dla systemu informacyjnego uczelni wyższej.

Wykres 3.11. przedstawia odpowiedzi respondentów grupy kadra administracyjna i grupy studenci (różne kierunki) na temat stopnia zagrożenia systemu uczelni wyższej przez utratę danych.

Wykres 3.11. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy studenci (różne kierunki) na temat stopnia zagrożenia systemu uczelni wyższej przez utratę danych



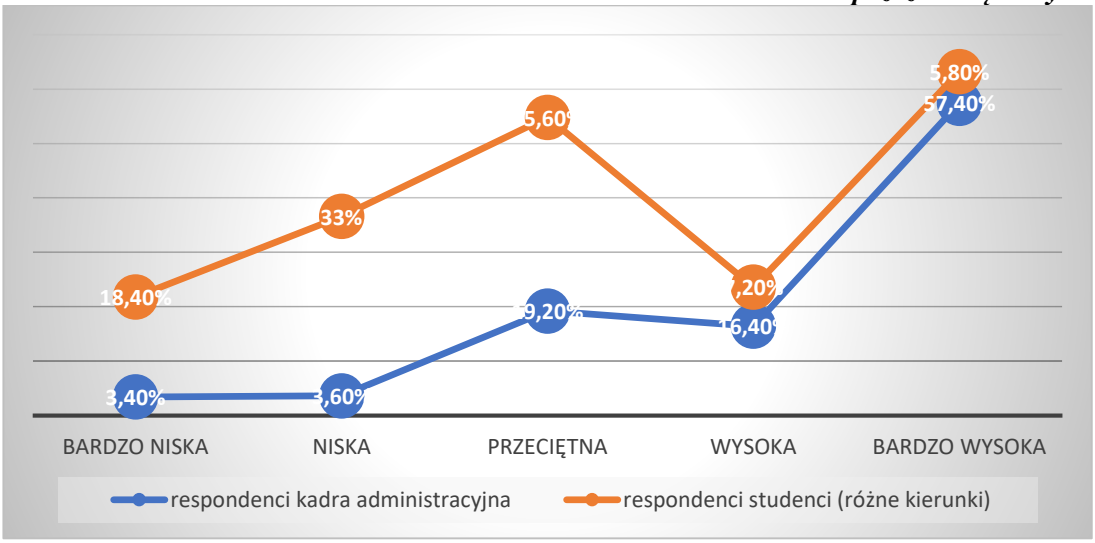
Źródło: opracowanie własne na podstawie badań własnych

O stopniu zależności świadczy współczynnik korelacji liniowej Pearsona na poziomie -0,55 i współczynnik determinacji liniowej, który wskazuje procent wyjaśnionej liniowo zmienności równy 30,25%. Wykres 3.12. pokazuje zależność między respondentami grupy kadra administracyjna i grupy studenci (różne kierunki) pod względem stopnia zagrożenia systemu uczelni wyższej przez utratę danych.

$$r_{xy} = \frac{\frac{1}{n}\sum_{i=1}^{n}(x_i-\bar{x})(y_i-\bar{y})}{S_x S_y}\text{=-0,55}$$

$$\text{WD=r}\frac{2}{xy} * 100\% = 30{,}25\%$$

Wykres 3.12. Zależność między respondentami grupy kadra administracyjna i grupy studenci (różne kierunki) pod względem stopnia zagrożenia systemu uczelni wyższej przez utratę danych



Źródło: opracowanie własne na podstawie badań własnych

W związku z faktem, że wartość liczbowa w ocenie relacji jest ujemna oznacza to, iż wraz ze wzrostem wartości jednej zmiennej maleje wartość drugiej.

13. Jak Państwo oceniają zagrożenia systemu informacyjnego w uczelni wyższej?

c) Zmiana hasła przez osoby trzecie i brak dostępu do własnego konta użytkownika

Rozkład odpowiedzi respondentów grupy nauczyciele akademiccy i grupy kadra administracyjna dotyczące oceny zmiany przez użytkowników stopnia zagrożenia systemu uczelni wyższej przez zmianę hasła przez osoby trzecie i brak dostępu do własnego konta użytkownika zostało zaprezentowane w tabeli 3.7.

Tabela 3.7. Odpowiedzi respondentów pracowników grupy nauczyciele akademiccy i grupy kadra administracyjna na temat zagrożeń systemu informacyjnego w uczelni wyższej przez zmianę hasła przez osoby trzecie i brak dostępu do własnego konta użytkownika

Odpowiedzi badanych osób zmiana hasła przez osoby trzecie i brak dostępu do własnego konta użytkownika						
Osoby poddane badaniu	**Respondenci nauczyciele akademiccy**		**Respondenci kadra administracyjna**		**OGÓŁEM**	
Ocena	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***
bardzo niska	15	3%	31	6,2%	46	4,6%
niska	159	31,8%	129	25,8%	288	28,8%
przeciętna	281	56,2%	312	62,4%	593	59,3%
wysoka	25	5%	12	2,4%	37	3,7%
bardzo wysoka	20	4%	16	3,2%	36	3,6%
	500	**100%**	**500**	**100%**	**1000**	**100%**

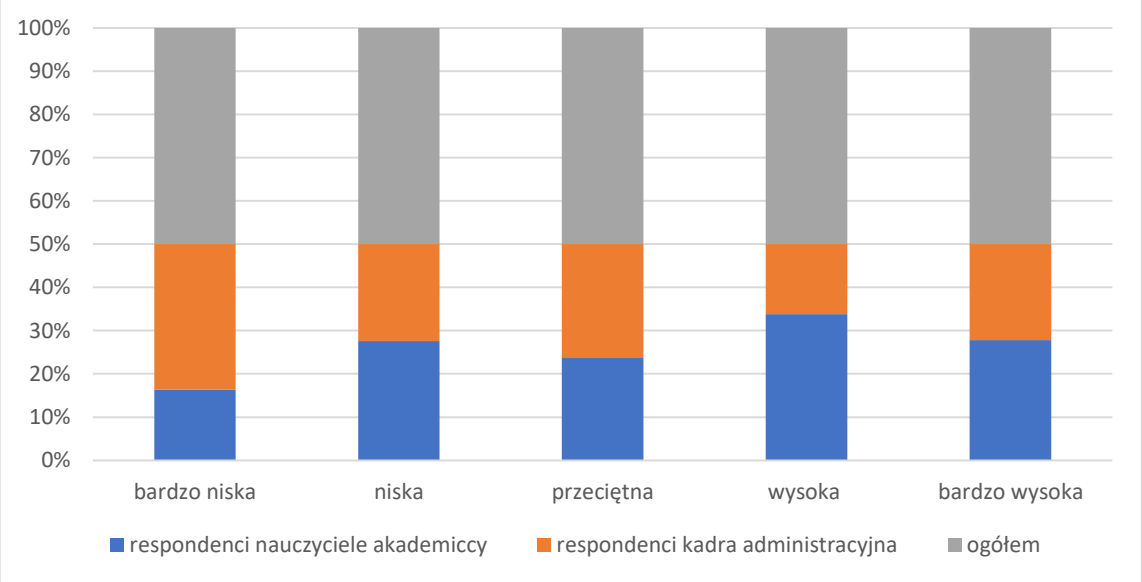
Źródło: opracowanie własne na podstawie badań własnych

W badaniu wzięło udział 500 osób zatrudnionych na stanowisku, nauczycieli akademickich oraz 500 osób zatrudnionych na stanowisku kadra administracyjna. Z przeprowadzonej analizy wynika, że nauczyciele akademiccy jak i kadra administracyjna ocenili stopień zagrożenia systemu uczelni wyższej dotyczącą zmiany hasła przez osoby trzecie i brak dostępu do własnego konta użytkownika, jako przeciętny. Wskazuje na to 281 respondentów, co w udziale procentowym wynosi 56,2% dla nauczycieli akademickich i 312 respondentów, co w udziale procentowym dla kadry administracyjnej wynosi 62,4%.

Analizując udzielone odpowiedzi w opinii 15 respondentów, co w udziale procentowym wynosi 3% dla nauczycieli akademickich i 31 respondentów, co w udziale procentowym daje 6,2% dla kadry administracyjnej świadczy, że pojawienie się zmiany hasła przez osoby trzecie i brak dostępu do własnego konta użytkownika stanowi bardzo małe zagrożenie dla systemu informacyjnego uczelni wyższej.

Wykres 3.13. przedstawia odpowiedzi respondentów grupy nauczyciele akademiccy i grupy kadra administracyjna na temat stopnia zagrożenia systemu uczelni wyższej przez zmiany hasła przez osoby trzecie i brak dostępu do własnego konta użytkownika.

Wykres 3.13. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy kadra administracyjna na temat stopnia zagrożenia systemu uczelni wyższej przez zmiany hasła przez osoby trzecie i brak dostępu do własnego konta użytkownika



Źródło: opracowanie własne na podstawie badań własnych

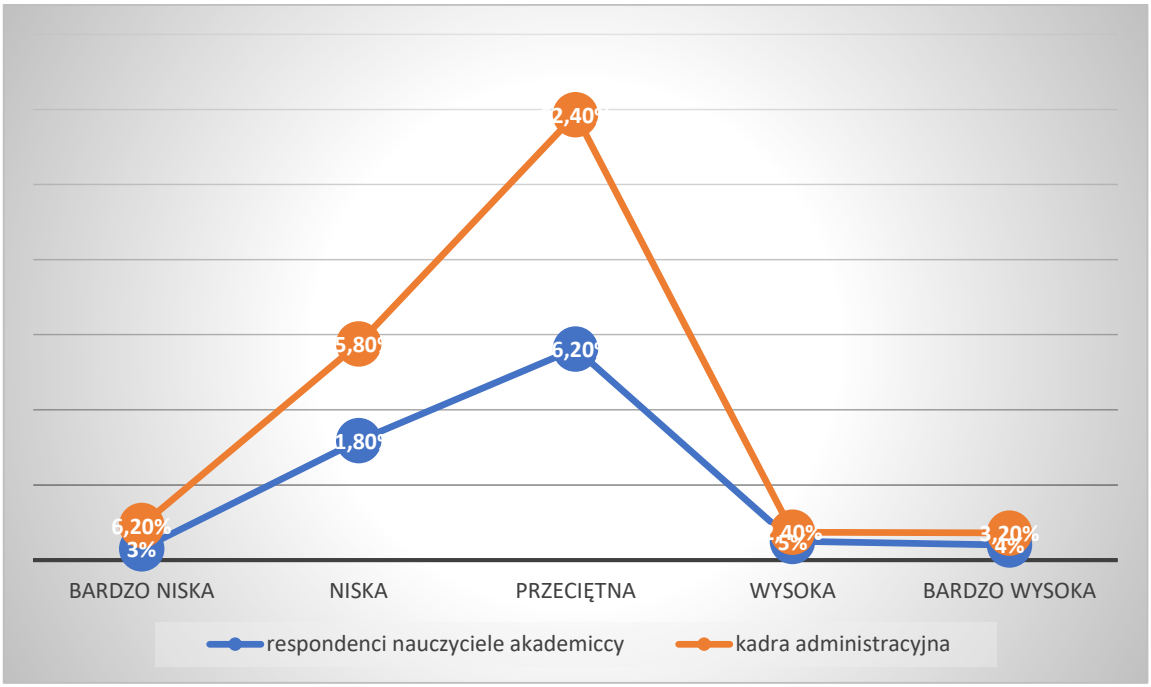
O stopniu zależności świadczy współczynnik korelacji liniowej Pearsona na poziomie 0,98 i współczynnik determinacji liniowej, który wskazuje procent wyjaśnionej

liniowo zmienności równy 96,4%. Wykres 3.14. pokazuje zależność między respondentami grupy nauczyciele akademiccy i grupy kadra administracyjna pod względem stopnia zagrożenia systemu uczelni wyższej w wyniku zmiany hasła przez osoby trzecie i brak dostępu do własnego konta użytkownika.

$$r_{xy} = \frac{\frac{1}{n}\sum_{i=1}^{n}(x_i-\bar{x})(y_i-\bar{y})}{S_x S_y}=0{,}98$$

$$\text{WD}=r_{xy}^{2} * 100\% = 96{,}4\%$$

Wykres 3.14. Zależność między respondentami grupy nauczyciele akademiccy i kadra administracyjna pod względem stopnia zagrożenia systemu uczelni wyższej w wyniku zmiany hasła przez osoby trzecie i brak dostępu do własnego konta użytkownika



Źródło: opracowanie własne na podstawie badań własnych

W związku z faktem, że wartość liczbowa w ocenie relacji jest dodatnia oznacza to, iż wraz ze wzrostem wartości jednej zmiennej rosną wartości także drugiej. Tabela 3.8. przedstawia odpowiedzi respondentów grupy nauczyciele akademiccy i grupy studenci (różne kierunki) na temat zagrożeń systemu informacyjnego w uczelni wyższej w wyniku zmiany hasła przez osoby trzecie i brak dostępu do własnego konta użytkownika.

Tabela 3.8. Odpowiedzi respondentów pracowników grupy nauczyciele akademiccy i grupy studenci (różne kierunki) na temat zagrożeń systemu informacyjnego w uczelni wyższej w wyniku zmiany hasła przez osoby trzecie i brak dostępu do własnego konta użytkownika

Odpowiedzi badanych osób zmiana hasła przez osoby trzecie i brak dostępu do własnego konta użytkownika						
Osoby poddane badaniu	**Respondenci nauczyciele akademiccy**		**Respondenci studenci (różne kierunki)**		**OGÓŁEM**	
Ocena	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***
bardzo niska	15	3%	17	3,4%	32	3,2%
niska	159	31,8%	83	16,6%	242	24,2%
przeciętna	281	56,2%	362	72,4%	643	64,3%
wysoka	25	5%	34	6,8%	59	5,9%
bardzo wysoka	20	4%	4	0,8%	24	2,4%
	500	**100%**	**500**	**100%**	**1000**	**100%**

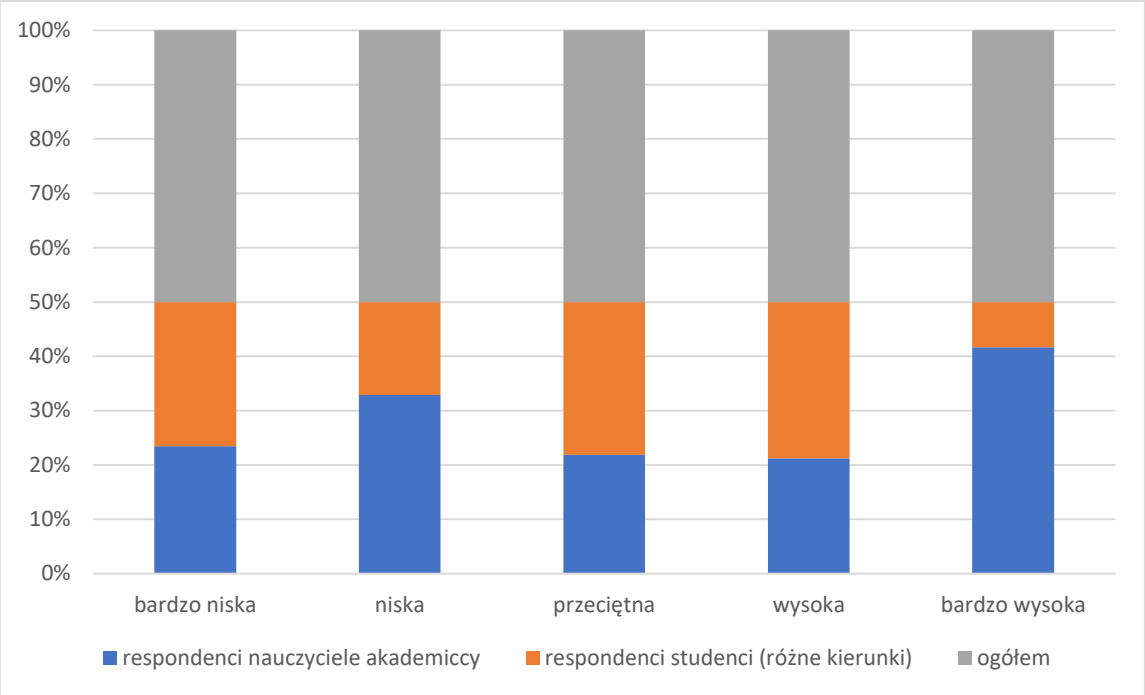
Źródło: opracowanie własne na podstawie badań własnych

W badaniu wzięło udział 500 osób zatrudnionych na stanowisku, nauczycieli akademickich oraz 500 osób studiujących w uczelni wyższej. Z przeprowadzonej analizy wynika, że nauczyciele akademiccy jak i studenci (różne kierunki) ocenili stopień zagrożenia systemu uczelni wyższej w wyniku zmiany hasła przez osoby trzecie i brak dostępu do własnego konta użytkownika, jako przeciętny. Wskazuje na to 281 respondentów, co w udziale procentowym wynosi 56,2% dla nauczycieli akademickich i 362 respondentów, co w udziale procentowym dla studentów (różne roczniki) wynosi 72,4%.

Analizując udzielone odpowiedzi w opinii 20 respondentów, co w udziale procentowym wynosi 4% dla nauczycieli akademickich i 4 respondentów, co w udziale procentowym daje 0,8% dla studentów studiujących w uczelni wyższej świadczy, że pojawienie się zmiany hasła przez osoby trzecie i brak dostępu do własnego konta użytkownika stanowi bardzo duże zagrożenie dla systemu informacyjnego uczelni wyższej.

Wykres 3.15. przedstawia odpowiedzi respondentów grupy nauczyciele akademiccy i grupy studenci (różne kierunki) na temat stopnia zagrożenia systemu uczelni wyższej w wyniku zmiany hasła przez osoby trzecie i brak dostępu do własnego konta użytkownika.

Wykres 3.15. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy studenci (różne kierunki) na temat stopnia zagrożenia systemu uczelni wyższej w wyniku zmiany hasła przez osoby trzecie i brak dostępu do własnego konta użytkownika



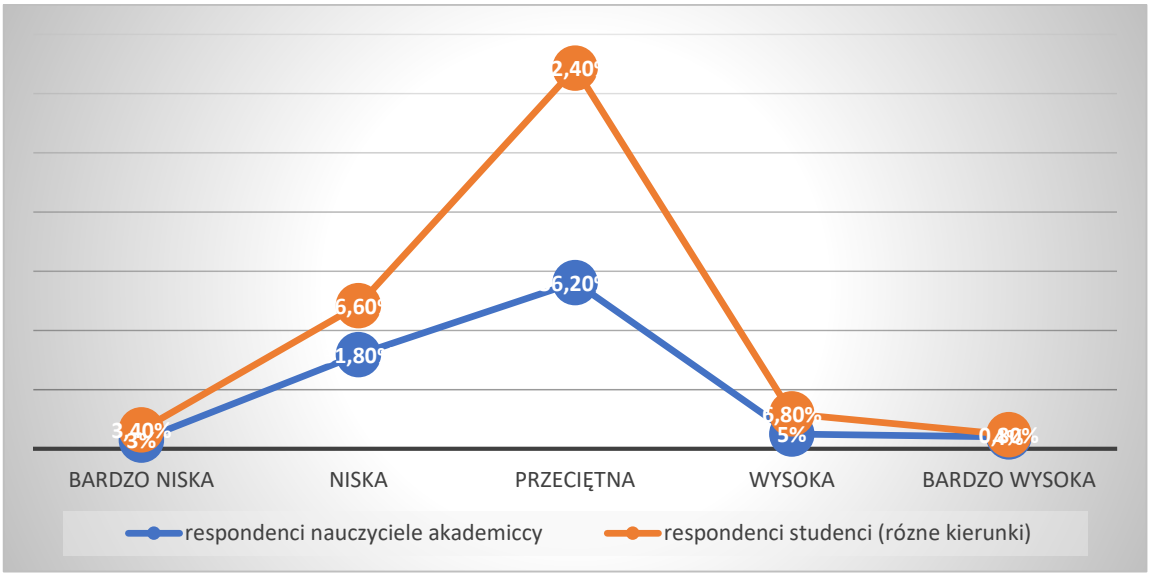
Źródło: opracowanie własne na podstawie badań własnych

O stopniu zależności świadczy współczynnik korelacji liniowej Pearsona na poziomie 0,94 i współczynnik determinacji liniowej, który wskazuje procent wyjaśnionej liniowo zmienności równy 88,36%. Wykres 3.16. pokazuje zależność między respondentami grupy nauczyciele akademiccy i grupy studenci (różne kierunki) pod względem stopnia zagrożenia systemu uczelni wyższej w wyniku zmiany hasła przez osoby trzecie i brak dostępu do własnego konta użytkownika.

$$r_{xy} = \frac{\frac{1}{n}\sum_{i=1}^{n}(x_i-\bar{x})(y_i-\bar{y})}{S_x S_y}=0{,}94$$

$$\mathrm{WD}=r_{xy}^{2} * 100\% = 88{,}36\%$$

Wykres 3.16. Zależność między respondentami grupy nauczyciele akademiccy i grupy studenci (różne kierunki) pod względem stopnia zagrożenia systemu uczelni wyższej w wyniku zmiany hasła przez osoby trzecie i brak dostępu do własnego konta użytkownika



Źródło: opracowanie własne na podstawie badań własnych

W związku z faktem, że wartość liczbowa w ocenie relacji jest dodatnia oznacza to, iż wraz ze wzrostem wartości jednej zmiennej rosną wartości także drugiej. Tabela 3.9. przedstawia odpowiedzi respondentów grupy kadra administracyjna i grupy studenci (różne kierunki) na temat zagrożeń systemu informacyjnego w uczelni wyższej w wyniku zmiany hasła przez osoby trzecie i brak dostępu do własnego konta użytkownika.

Tabela 3.9. Odpowiedzi respondentów pracowników grupy kadra administracyjna i grupy studenci (różne kierunki) na temat zagrożeń systemu informacyjnego w uczelni wyższej w wyniku zmiany hasła przez osoby trzecie i brak dostępu do własnego konta użytkownika

Odpowiedzi badanych osób zmiana hasła przez osoby trzecie i brak dostępu do własnego konta użytkownika						
Osoby poddane badaniu	**Respondenci kadra administracyjna**		**Respondenci studenci (różne kierunki)**		**OGÓŁEM**	
Ocena	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***
bardzo niska	31	6,2%	17	3,4%	48	4,8%
niska	129	25,8%	83	16,6%	212	21,2%
przeciętna	312	62,4%	362	72,4%	674	67,4%
wysoka	12	2,4%	34	34%	46	4,6%
bardzo wysoka	16	3,2%	4	0,8%	20	2%
	500	**100%**	**500**	**100%**	**1000**	**100%**

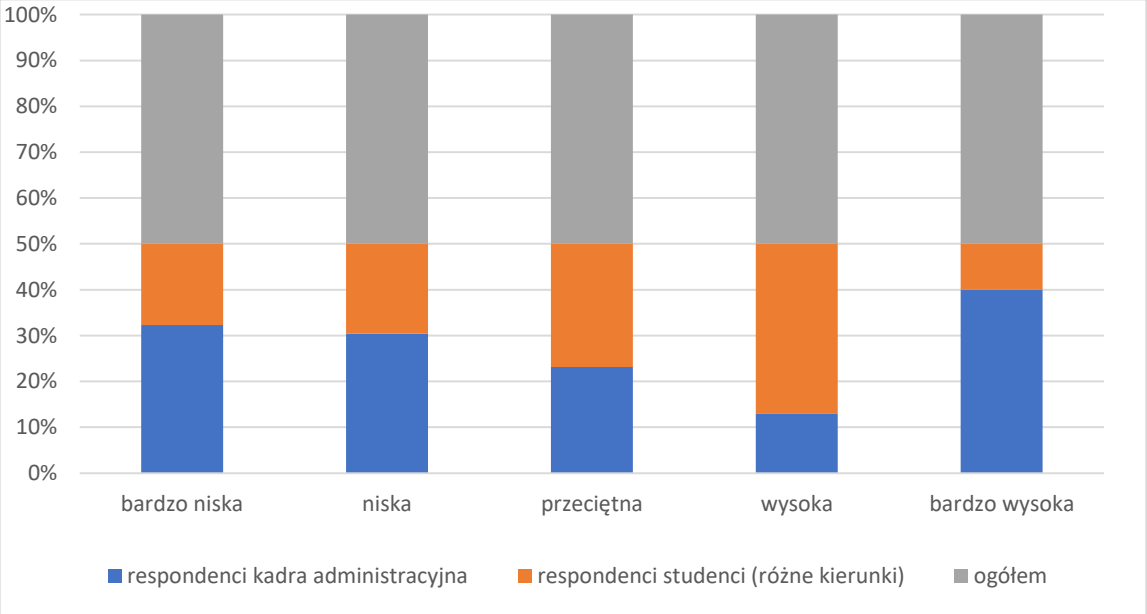
Źródło: opracowanie własne na podstawie badań własnych

W badaniu wzięło udział 500 osób zatrudnionych na stanowisku, kadry administracyjnej oraz 500 osób studiujących w uczelni wyższej. Z przeprowadzonej analizy wynika, że kadra administracyjna jak i studenci (różne kierunki) ocenili stopień zagrożenia systemu uczelni wyższej, w wyniku zmiany hasła przez osoby trzecie i brak dostępu do własnego konta użytkownika, jako przeciętny. Wskazuje na to 312 respondentów, co w udziale procentowym wynosi 62,4% dla kadry administracyjnej i 362 respondentów, co w udziale procentowym dla studentów (różne roczniki) wynosi 72,4%.

Analizując udzielone odpowiedzi w opinii 16 respondentów, co w udziale procentowym wynosi 3,2% dla kadry administracyjnej i 4 respondentów, co w udziale procentowym daje 0,8% dla studentów studiujących w uczelni wyższej świadczy, że pojawienie się klęski żywiołowej stanowi bardzo duże zagrożenie dla systemu informacyjnego uczelni wyższej.

Wykres 3.17. przedstawia odpowiedzi respondentów grupy kadra administracyjna i grupy studenci (różne kierunki) na temat stopnia zagrożenia systemu uczelni wyższej w wyniku zmiany hasła przez osoby trzecie i brak dostępu do własnego konta użytkownika.

Wykres 3.17. Odpowiedzi respondentów grupy kadra administracyjna i grupy studenci (różne kierunki) na temat stopnia zagrożenia systemu uczelni wyższej w wyniku zmiany hasła przez osoby trzecie i brak dostępu do własnego konta użytkownika



Źródło: opracowanie własne na podstawie badań własnych

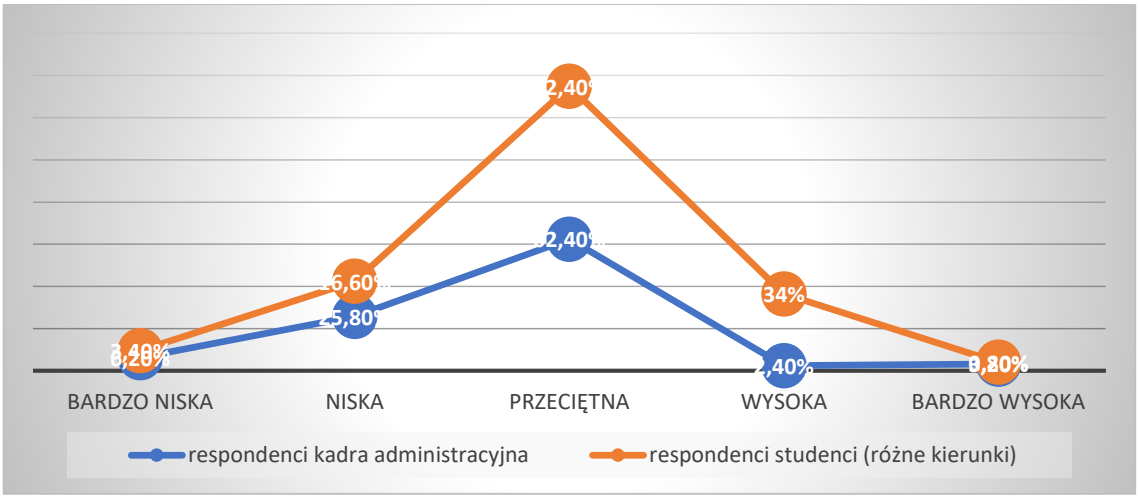
O stopniu zależności świadczy współczynnik korelacji liniowej Pearsona na poziomie 0,98 i współczynnik determinacji liniowej, który wskazuje procent wyjaśnionej liniowo zmienności równy 96,04%.

Wykres 3.18. pokazuje zależność między respondentami grupy kadra administracyjna i grupy studenci (różne kierunki) pod względem stopnia zagrożenia systemu uczelni wyższej w wyniku zmiany hasła przez osoby trzecie i brak dostępu do własnego konta użytkownika.

$$r_{xy} = \frac{\frac{1}{n}\sum_{i=1}^{n}(x_i-\bar{x})(y_i-\bar{y})}{S_x S_y}=0{,}98$$

$$\text{WD}=r_{xy}^{2} * 100\% = 96{,}04\%$$

Wykres 3.18. Zależność między respondentami grupy kadra administracyjna i grupy studenci (różne kierunki) pod względem stopnia zagrożenia systemu uczelni wyższej w wyniku zmiany hasła przez osoby trzecie i brak dostępu do własnego konta użytkownika



Źródło: opracowanie własne na podstawie badań własnych

W związku z faktem, że wartość liczbowa w ocenie relacji jest dodatnia oznacza to, iż wraz ze wzrostem wartości jednej zmiennej rosną wartości także drugiej.

13. Jak Państwo oceniają zagrożenia systemu informacyjnego w uczelni wyższej? d) Rozkodowywanie hasła dostępu

Rozkład odpowiedzi respondentów grupy nauczyciele akademiccy i kadra administracyjna dotyczący oceny przez użytkowników stopnia zagrożenia systemu uczelni wyższej przez rozkodowywanie hasła dostępu prezentuje tabela 3.10.

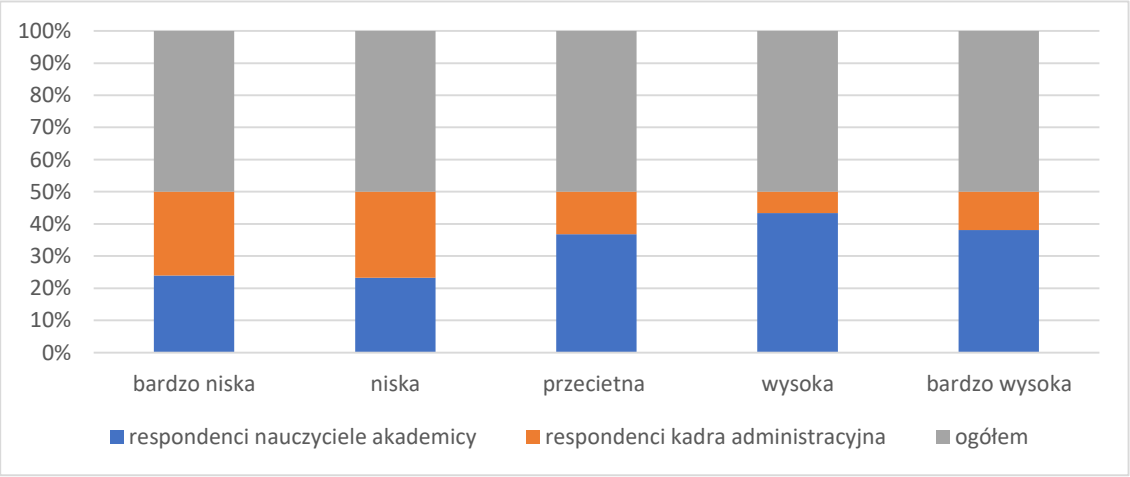
Tabela 3.10. Odpowiedzi respondentów pracowników nauczyciele akademiccy i grupy kadra naukowa na temat zagrożeń systemu informacyjnego w uczelni wyższej przez rozkodowanie hasła dostępu

Odpowiedzi badanych osób rozkodowanie hasła dostępu						
Osoby poddane badaniu	**Respondenci nauczyciele akademiccy**		**Respondenci kadra administracyjna**		**OGÓŁEM**	
Ocena	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***
bardzo niska	265	53%	289	57,8%	554	55,4%
niska	169	33,8%	195	39%	364	36,4%
przeciętna	25	5%	9	1,8%	34	3,4%
wysoka	26	5,2%	4	0,8%	30	3%
bardzo wysoka	16	3,2%	5	1%	21	2,1%
	500	**100%**	**500**	**100%**	**1000**	**100%**

Źródło: opracowanie własne na podstawie badań własnych

W badaniu wzięło udział 500 osób zatrudnionych na stanowisku, nauczycieli akademickich oraz 500 osób zatrudnionych na stanowisku kadry administracyjnej. Z przeprowadzonej analizy wynika, że nauczyciele akademiccy jak i kadra administracyjna, ocenili stopień zagrożenia systemu uczelni wyższej przez rozkodowanie hasła dostępu, jako bardzo niski. Wskazuje na to 265 respondentów, co w udziale procentowym wynosi 53% dla nauczycieli akademickich i 289 respondentów, co w udziale procentowym dla kadry administracyjnej wynosi 57,8%.

Wykres 3.19. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy kadra administracyjna na temat stopnia zagrożenia systemu uczelni wyższej poprzez rozkodowanie hasła dostępu



Źródło: opracowanie własne na podstawie badań własnych

Analizując udzielone odpowiedzi w opinii 16 respondentów, co w udziale procentowym wynosi 3,2% dla nauczycieli akademickich i 5 respondentów, co w udziale procentowym daje 1% dla kadry administracyjnej świadczy, że pojawienie się rozkodowania

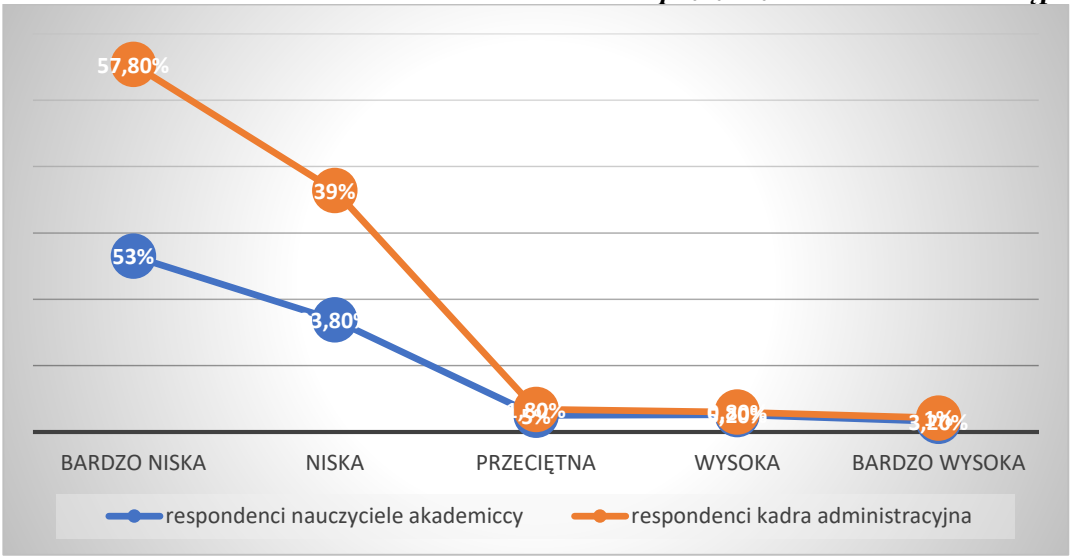
hasła dostępu stanowi bardzo duże zagrożenie dla systemu informacyjnego uczelni wyższej. Wykres 3.19. przedstawia odpowiedzi respondentów grupy nauczyciele akademiccy i grupy kadra administracyjna na temat stopnia zagrożenia systemu uczelni wyższej przez rozkodowanie hasła dostępu.

O stopniu zależności świadczy współczynnik korelacji liniowej Pearsona na poziomie 0,99 i współczynnik determinacji liniowej, który wskazuje procent wyjaśnionej liniowo zmienności równy 98,01%. Wykres 3.20. pokazuje zależność między respondentami grupy nauczyciele akademiccy i grupy kadra administracyjna pod względem stopnia zagrożenia systemu uczelni wyższej przez rozkodowanie hasła dostępu.

$$r_{xy} = \frac{\frac{1}{n}\sum_{i=1}^{n}(x_i-\bar{x})(y_i-\bar{y})}{S_x S_y}=0{,}99$$

$$\text{WD}=r_{xy}^{2} * 100\% = 98{,}01\%$$

Wykres 3.20. Zależność między respondentami grupy nauczyciele akademiccy i grupy kadra administracyjna pod względem stopnia zagrożenia systemu uczelni wyższej przez rozkodowanie hasła dostępu



Źródło: opracowanie własne na podstawie badań własnych

W związku z faktem, że wartość liczbowa w ocenie relacji jest dodatnia oznacza to, iż wraz ze wzrostem wartości jednej zmiennej rosną wartości także drugiej. Tabela 3.11. przedstawia odpowiedzi respondentów grupy nauczyciele akademiccy i grupy studenci (różne kierunki) na temat zagrożeń systemu informacyjnego w uczelni wyższej przez rozkodowanie hasła dostępu.

Tabela 3.11. Odpowiedzi respondentów pracowników nauczyciele akademiccy i grupy studenci (różne kierunki) na temat zagrożeń systemu informacyjnego w uczelni wyższej przez rozkodowanie hasła dostępu

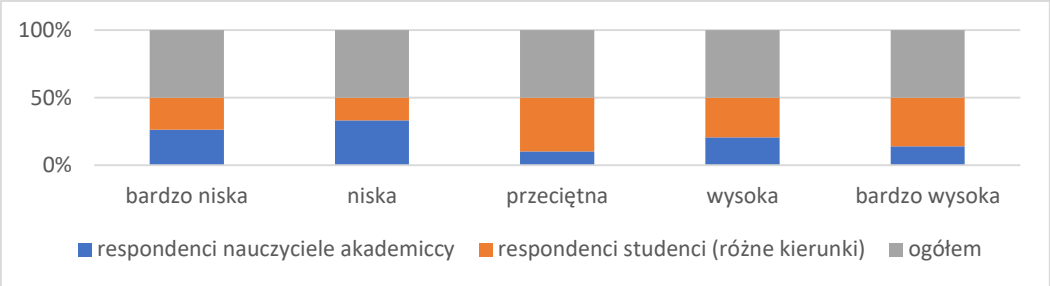
Odpowiedzi badanych osób rozkodowanie hasla dostępu						
Osoby poddane badaniu	**Respondenci nauczyciele akademiccy**		**Respondenci studenci (różne kierunki)**		**OGÓŁEM**	
Ocena	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***
bardzo niska	265	53%	238	47,6%	503	50,3%
niska	169	33,8%	85	17%	254	25,4%
przeciętna	25	5%	99	19,8%	124	12,4%
wysoka	26	5,2%	37	7,4%	63	6,3%
bardzo wysoka	16	3,2%	41	8,2%	57	5,7%
	500	**100%**	**500**	**100%**	**1000**	**100%**

Źródło: opracowanie własne na podstawie badań własnych

W badaniu wzięło udział 500 osób zatrudnionych na stanowisku, nauczycieli akademickich oraz 500 osób studiujących w uczelni wyższej. Z przeprowadzonej analizy wynika, że nauczyciele akademiccy jak i studenci (różne kierunki) ocenili stopień zagrożenia systemu uczelni wyższej przez rozkodowanie hasła, jako bardzo niski. Wskazuje na to 265 respondentów, co w udziale procentowym wynosi 53% dla nauczycieli akademickich i 238 respondentów, co w udziale procentowym dla studentów (różne roczniki) wynosi 47,6%.

Analizując udzielone odpowiedzi w opinii 16 respondentów, co w udziale procentowym wynosi 3,2% dla nauczycieli akademickich i 41 respondentów, co w udziale procentowym daje 8,2% dla studentów studiujących w uczelni wyższej świadczy, że pojawienie się rozkodowania hasła dostępu stanowi bardzo duże zagrożenie dla systemu informacyjnego uczelni wyższej.

Wykres 3.21. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy studenci (różne kierunki) na temat stopnia zagrożenia systemu uczelni wyższej przez rozkodowanie hasła dostępu



Źródło: opracowanie własne na podstawie badań własnych

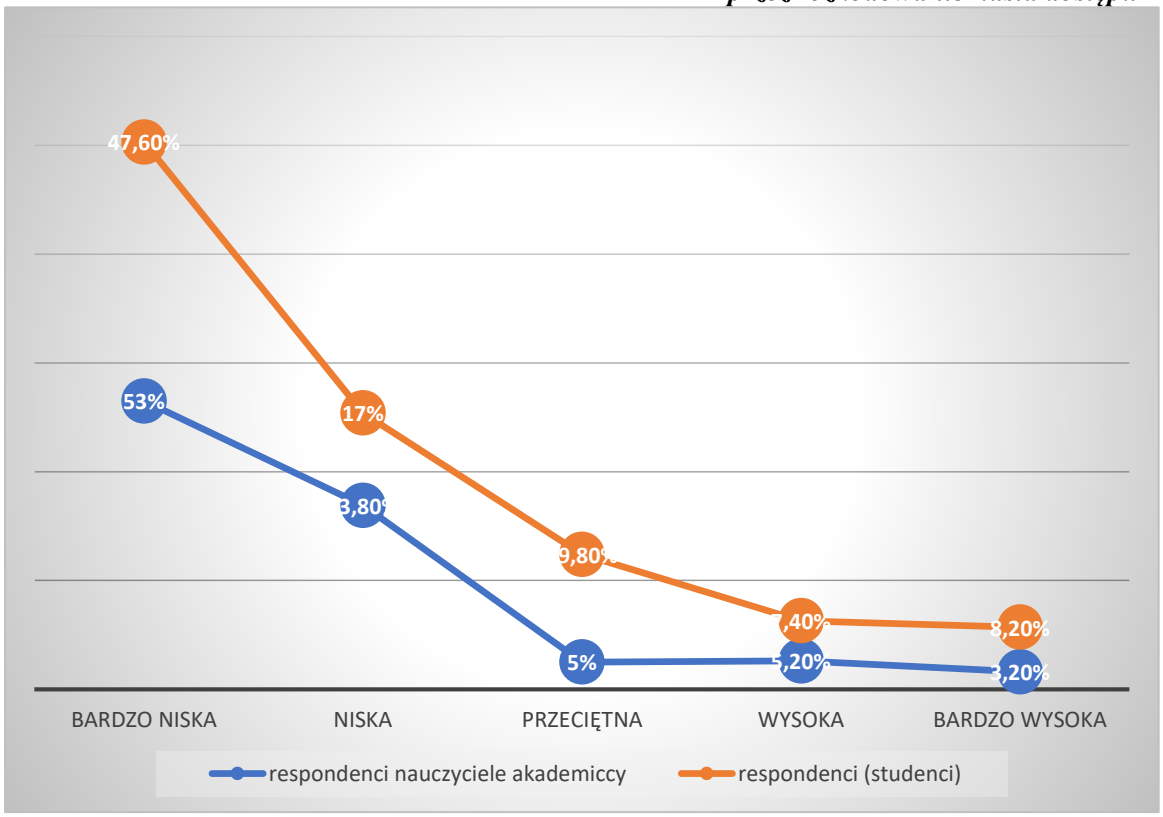
Wykres 3.21. przedstawia odpowiedzi respondentów grupy nauczyciele akademiccy i grupy studentów (różne kierunki) na temat stopnia zagrożenia systemu uczelni wyższej przez rozkodowanie hasła dostępu.

O stopniu zależności świadczy współczynnik korelacji liniowej Pearsona na poziomie 0,86 i współczynnik determinacji liniowej, który wskazuje procent wyjaśnionej liniowo zmienności równy 73,96%. Wykres 3.22. pokazuje zależność między respondentami grupy nauczyciele akademiccy i grupy studenci (różne kierunki) pod względem stopnia zagrożenia systemu uczelni wyższej przez rozkodowanie hasła dostępu.

$$r_{xy} = \frac{\frac{1}{n}\sum_{i=1}^{n}(x_i-\bar{x})(y_i-\bar{y})}{S_x S_y}=0{,}86$$

$$\text{WD}=r_{xy}^{2} * 100\% = 73{,}96\%$$

Wykres 3.22. Zależność między respondentami grupy nauczyciele akademiccy i grupy studenci (różne kierunki) pod względem stopnia zagrożenia systemu uczelni wyższej przez rozkodowanie hasła dostępu



Źródło: opracowanie własne na podstawie badań własnych

W związku z faktem, że wartość liczbowa w ocenie relacji jest dodatnia oznacza to, iż wraz ze wzrostem wartości jednej zmiennej rosną wartości także drugiej. Tabela

3.12. przedstawia odpowiedzi respondentów grupy kadra administracyjna i grupy studenci (różne kierunki) na temat zagrożeń systemu informacyjnego w uczelni wyższej przez rozkodowanie hasła dostępu.

Tabela 3.12. Odpowiedzi respondentów pracowników kadry administracyjnej i grupy studenci (różne kierunki) na temat zagrożeń systemu informacyjnego w uczelni wyższej przez rozkodowanie hasła dostępu

Odpowiedzi badanych osób rozkodowanie hasła dostępu						
Osoby poddane badaniu	**Respondenci kadra administracyjna**		**Respondenci studenci (różne kierunki)**		**OGÓŁEM**	
Ocena	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***
bardzo niska	289	57,8%	238	47,6%	527	52,7%
niska	195	39%	85	17%	280	28%
przeciętna	9	1,8%	99	19,8%	108	10,8%
wysoka	4	0,8%	37	7,4%	41	4,1%
bardzo wysoka	5	1%	41	8,2%	46	4,6%
	500	**100%**	**500**	**100%**	**1000**	**100%**

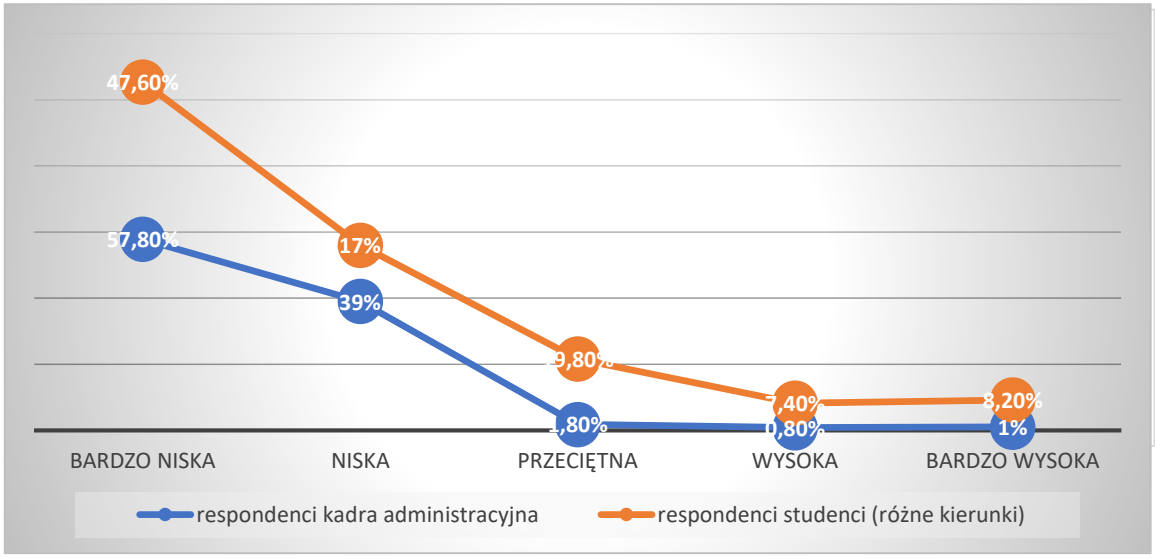
Źródło: opracowanie własne na podstawie badań własnych

W badaniu wzięło udział 500 osób zatrudnionych na stanowisku, kadra administracyjna oraz 500 osób studiujących w uczelni wyższej. Z przeprowadzonej analizy wynika, że kadra administracyjna jak i studenci (różne kierunki) ocenili stopień zagrożenia systemu uczelni wyższej przez rozkodowanie hasła dostępu, jako bardzo niski. Wskazuje na to 289 respondentów, co w udziale procentowym wynosi 57,8% dla kadry administracyjnej i 238 respondentów, co w udziale procentowym dla studentów (różne roczniki) wynosi 47,6%.

Analizując udzielone odpowiedzi w opinii 5 respondentów, co w udziale procentowym wynosi 1% dla kadry administracyjnej i 41 respondentów, co w udziale procentowym daje 8,2% dla studentów studiujących w uczelni wyższej świadczy, że pojawienie się rozkodowania hasła stanowi bardzo duże zagrożenie dla systemu informacyjnego uczelni wyższej.

Wykres 3.23. przedstawia odpowiedzi respondentów grupy kadra administracyjna i grupy studenci (różne kierunki) na temat stopnia zagrożenia systemu uczelni wyższej przez rozkodowanie hasła dostępu.

Wykres 3.23. Odpowiedzi respondentów grupy kadra administracyjna i grupy studenci (różne kierunki) na temat stopnia zagrożenia systemu uczelni wyższej przez rozkodowanie hasła dostępu



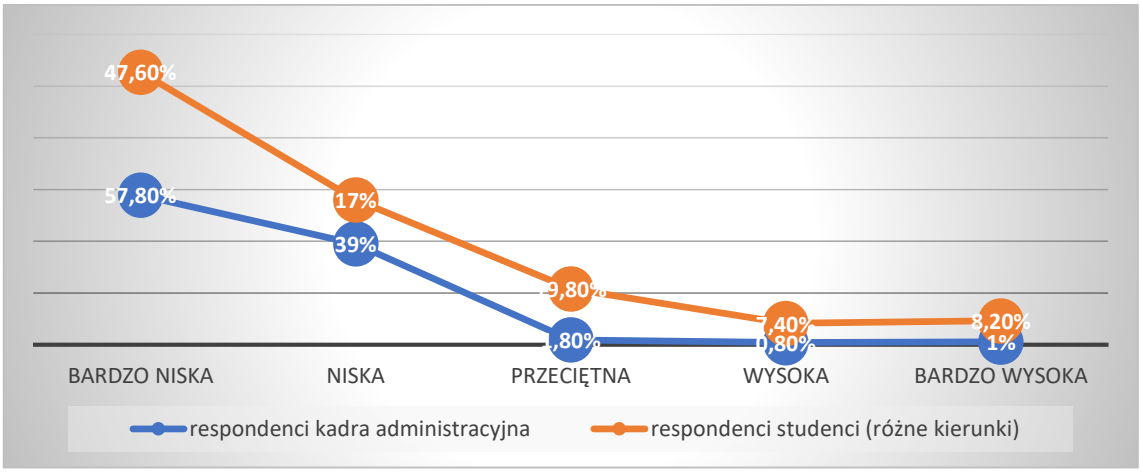
Źródło: opracowanie własne na podstawie badań własnych

O stopniu zależności świadczy współczynnik korelacji liniowej Pearsona na poziomie 0,83 i współczynnik determinacji liniowej, który wskazuje procent wyjaśnionej liniowo zmienności równy 68,89%. Wykres 3.24. pokazuje zależność między respondentami grupy kadra administracyjna i grupy studenci (różne kierunki) pod względem stopnia zagrożenia systemu uczelni wyższej przez rozkodowanie hasła dostępu.

$$r_{xy} = \frac{\frac{1}{n}\sum_{i=1}^{n}(x_i-\bar{x})(y_i-\bar{y})}{S_x S_y}=0{,}83$$

$$\mathrm{WD}=r_{xy}^{2} * 100\% = 68{,}89\%$$

Wykres 3.24. Zależność między respondentami grupy kadra administracyjna i grupy studenci (różne kierunki) pod względem stopnia zagrożenia systemu uczelni wyższej przez rozkodowanie hasła dostępu



Źródło: opracowanie własne na podstawie badań własnych

W związku z faktem, że wartość liczbowa w ocenie relacji jest dodatnia oznacza to, iż wraz ze wzrostem wartości jednej zmiennej rosną wartości także drugiej.

13. Jak Państwo oceniają zagrożenia systemu informacyjnego w uczelni wyższej?
e) Cyberatak

Rozkład odpowiedzi respondentów grupy nauczyciele akademiccy i grupy kadra administracyjna dotyczący oceny przez użytkowników stopnia zagrożenia systemu w uczelni wyższej przez cyberatak zaprezentowano w tabeli 3.13.

Tabela 3.13. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy kadra administracyjna na temat zagrożeń systemu informacyjnego w uczelni wyższej przez cyberatak

Odpowiedzi badanych osób cyberatak						
Osoby poddane badaniu	**Respondenci nauczyciele akademiccy**		**Respondenci kadra administracyjna**		**OGÓŁEM**	
Ocena	*liczba wskazań*	*udział procentowy*	*liczba wskazań*	*udział procentowy*	*liczba wskazań*	*udział procentowy*
bardzo niska	412	82,4%	389	77,8%	801	80,1%
niska	35	7%	42	8,4%	77	7,7%
przeciętna	18	3,6%	26	5,2%	44	4,4%
wysoka	19	3,8%	24	4,8%	43	4,3%
bardzo wysoka	16	3,2%	19	3,8%	35	3,5%
	500	**100%**	**500**	**100%**	**1000**	**100%**

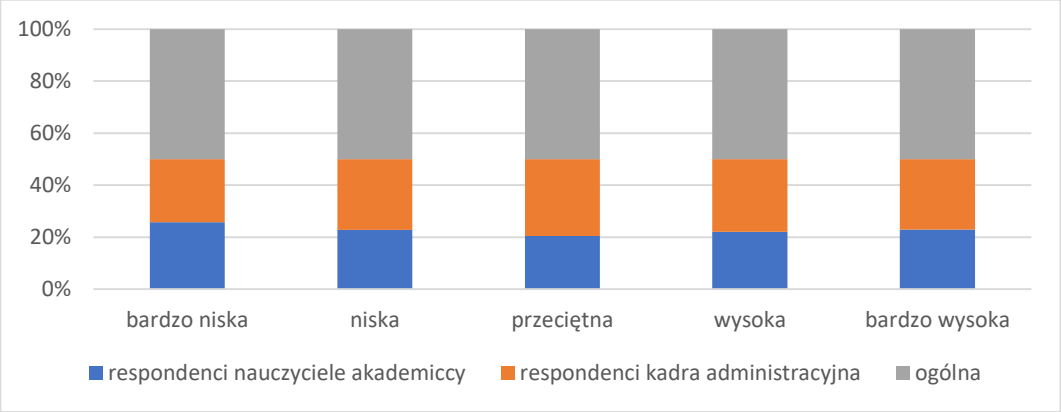
Źródło: opracowanie własne na podstawie badań własnych

W badaniu wzięło udział 500 osób zatrudnionych na stanowisku, nauczycieli akademickich oraz 500 osób zatrudnionych na stanowisku kadra administracyjna. Z przeprowadzonej analizy wynika, że nauczyciele akademiccy jak i kadra administracyjna ocenili stopień zagrożenia systemu uczelni wyższej przez cyberatak, jako bardzo niski. Wskazuje na to 412 respondentów, co w udziale procentowym wynosi 82,4% dla nauczycieli akademickich i 389 respondentów, co w udziale procentowym dla kadry administracyjnej wynosi 77,8%.

Analizując udzielone odpowiedzi w opinii 16 respondentów, co w udziale procentowym wynosi 3,2% dla nauczycieli akademickich i 19 respondentów, co w udziale procentowym daje 3,8% dla kadry administracyjnej świadczy, że pojawienie się cyberataku stanowi bardzo duże zagrożenie dla systemu informacyjnego uczelni wyższej.

Wykres 3.25. przedstawia odpowiedzi respondentów grupy nauczyciele akademiccy i grupy kadra administracyjna na temat stopnia zagrożenia systemu uczelni wyższej przez cyberatak.

Wykres 3.25. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy kadra administracyjna na temat stopnia zagrożenia systemu uczelni wyższej przez cyberatak



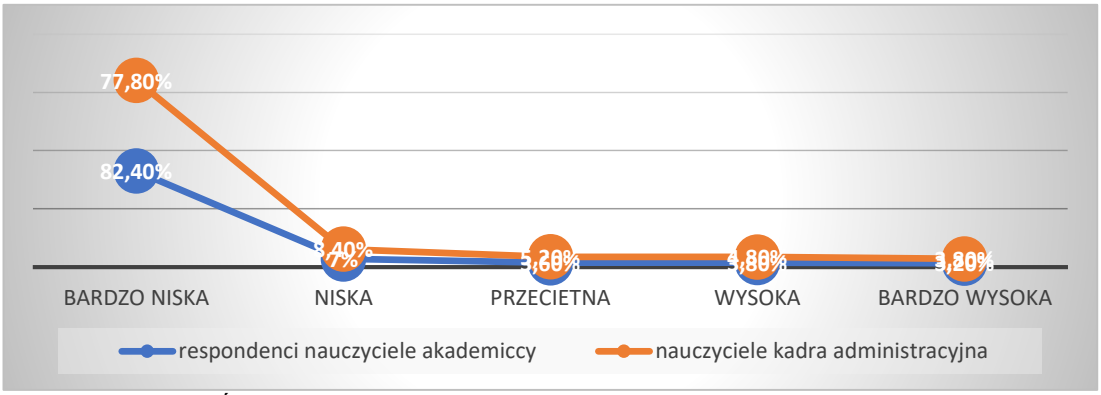
Źródło: opracowanie własne na podstawie badań własnych

O stopniu zależności świadczy współczynnik korelacji liniowej Pearsona na poziomie 1 i współczynnik determinacji liniowej, który wskazuje procent wyjaśnionej liniowo zmienności równy 100%. Wykres 3.26. pokazuje zależność między respondentami grupy nauczyciele akademiccy i grupy kadra administracyjna pod względem stopnia zagrożenia systemu uczelni wyższej przez cyberatak.

$$r_{xy} = \frac{\frac{1}{n}\sum_{i=1}^{n}(x_i-\bar{x})(y_i-\bar{y})}{S_x S_y}=1$$

$$WD=r\frac{2}{xy} * 100\% = 100\%$$

Wykres 3.26. Zależność między respondentami grupy nauczyciele akademiccy i grupy kadra administracyjna pod względem stopnia zagrożenia systemu uczelni wyższej przez cyberatak



Źródło: opracowanie własne na podstawie badań własnych

W związku z faktem, że wartość liczbowa w ocenie relacji jest dodatnia oznacza to, iż wraz ze wzrostem wartości jednej zmiennej rosną wartości także drugiej. Tabela 3.14. przedstawia odpowiedzi respondentów grupy nauczyciele akademiccy i grupy studenci (różne kierunki) na temat zagrożeń systemu informacyjnego w uczelni wyższej przez cyberatak.

Tabela. 3.14. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy studenci (różne kierunki) na temat zagrożeń systemu informacyjnego w uczelni wyższej przez cyberatak

Odpowiedzi badanych osób cyberatak						
Osoby poddane badaniu	**Respondenci nauczyciele akademiccy**		**Respondenci studenci (różne kierunki)**		**OGÓŁEM**	
Ocena	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***
bardzo niska	412	82,4%	289	57,8%	701	70,1%
niska	35	7%	115	23%	150	15%
przeciętna	18	3,6%	45	9%	63	6,3%
wysoka	19	3,8%	26	5,2%	45	4,5%
bardzo wysoka	16	3,2%	25	5%	41	4,1%
	500	**100%**	**500**	**100%**	**1000**	**100%**

Źródło: opracowanie własne na podstawie badań własnych

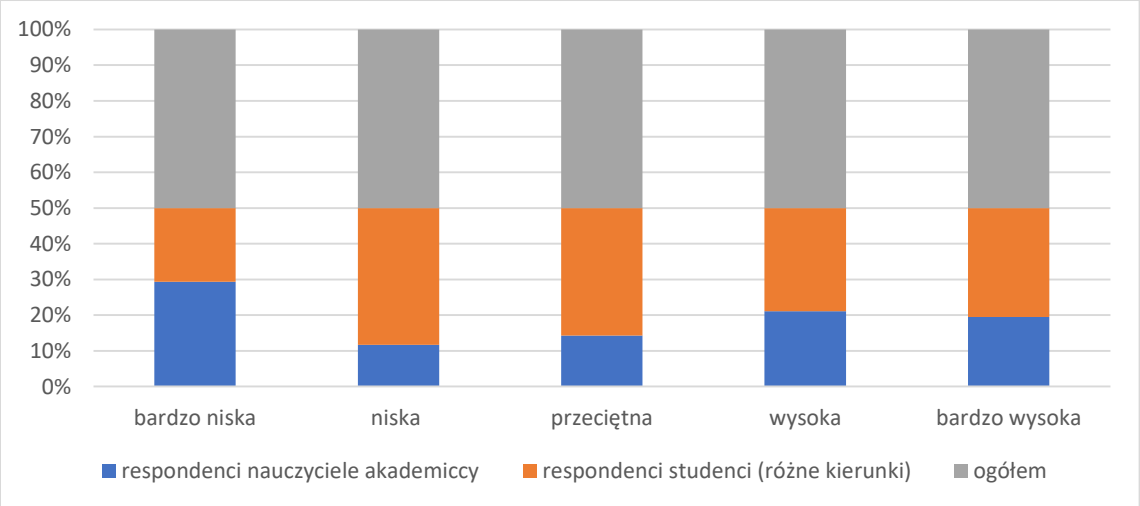
W badaniu wzięło udział 500 osób zatrudnionych na stanowisku, nauczycieli akademickich oraz 500 osób studiujących w uczelni wyższej. Z przeprowadzonej analizy

wynika, że nauczyciele akademiccy jak i studenci (różne kierunki) ocenili stopień zagrożenia systemu uczelni wyższej przez cyberatak, jako bardzo niski. Wskazuje na to 412 respondentów, co w udziale procentowym wynosi 82,4% dla nauczycieli akademickich i 289 respondentów, co w udziale procentowym dla studentów (różne roczniki) wynosi 57,8%.

Analizując udzielone odpowiedzi w opinii 16 respondentów, co w udziale procentowym wynosi 3,2% dla nauczycieli akademickich i 25 respondentów, co w udziale procentowym daje 5% dla studentów studiujących w uczelni wyższej świadczy, że pojawienie się cyberataku stanowi bardzo duże zagrożenie dla systemu informacyjnego uczelni wyższej.

Wykres 3.27. przedstawia odpowiedzi respondentów grupy nauczyciele akademiccy i grupy studentów (różne kierunki) na temat stopnia zagrożenia systemu uczelni wyższej przez cyberatak.

Wykres 3.27. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy studenci (różne kierunki) na temat stopnia zagrożenia systemu uczelni wyższej przez cyberatak



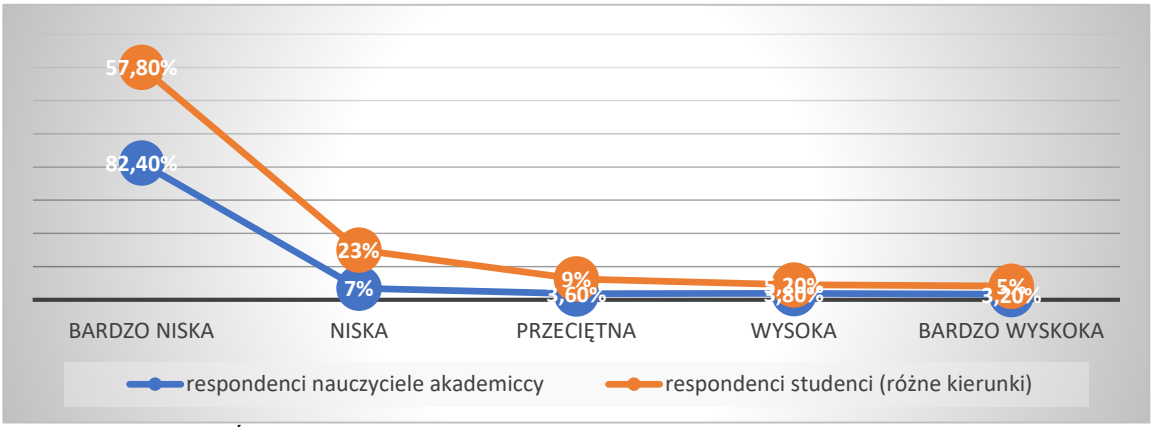
Źródło: opracowanie własne na podstawie badań własnych

O stopniu zależności świadczy współczynnik korelacji liniowej Pearsona na poziomie 0,96 i współczynnik determinacji liniowej, który wskazuje procent wyjaśnionej liniowo zmienności równy 92,16%. Wykres 3.28. pokazuje zależność między respondentami grupy nauczyciele akademiccy i grupy studenci (różne kierunki) pod względem stopnia zagrożenia systemu uczelni wyższej przez cyberatak.

$$r_{xy} = \frac{\frac{1}{n}\sum_{i=1}^{n}(x_i-\bar{x})(y_i-\bar{y})}{S_x S_y}=0{,}96$$

$$\text{WD}=r_{xy}^{2} * 100\% = 92{,}16\%$$

Wykres 3.28. Zależność między respondentami grupy nauczyciele akademiccy i grupy studenci (różne kierunki) pod względem stopnia zagrożenia systemu uczelni wyższej przez cyberatak



Źródło: opracowanie własne na podstawie badań własnych

W związku z faktem, że wartość liczbowa w ocenie relacji jest dodatnia oznacza to, iż wraz ze wzrostem wartości jednej zmiennej rosną wartości także drugiej. Tabela 3.15. przedstawia odpowiedzi respondentów grupy kadra administracyjna i grupy studenci (różne kierunki) na temat zagrożeń systemu informacyjnego w uczelni wyższej przez cyberatak.

Tabela 3.15. Odpowiedzi respondentów grupy kadra administracyjna i grupy studenci (różne kierunki) na temat zagrożeń systemu informacyjnego w uczelni wyższej przez cyberatak

Odpowiedzi badanych osób cyberatak						
Osoby poddane badaniu	**Respondenci kadra administracyjna**		**Respondenci studenci (różne kierunki)**		**OGÓŁEM**	
Ocena	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***
bardzo niska	389	77,8%	289	57,8%	678	67,8%
niska	42	8,4%	115	23%	157	15,7%
przeciętna	26	5,2%	45	9%	71	7,1%
wysoka	24	4,8%	26	5,2%	50	5
bardzo wysoka	19	3,8%	25	5%	44	4,4%
	500	**100%**	**500**	**100%**	**1000**	**100%**

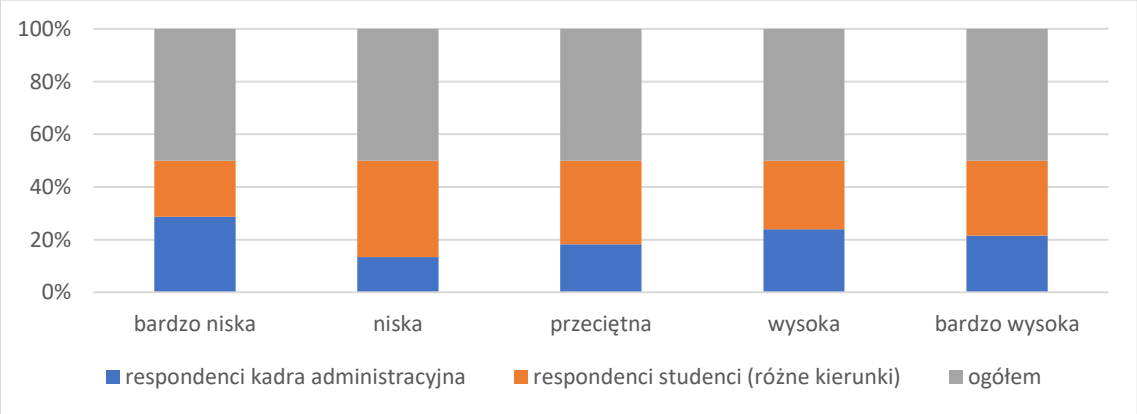
Źródło: opracowanie własne na podstawie badań własnych

W badaniu wzięło udział 500 osób zatrudnionych na stanowisku, kadry administracyjnej oraz 500 osób studiujących w uczelni wyższej. Z przeprowadzonej analizy wynika, że kadra administracyjna jak i studenci (różne kierunki) ocenili stopień zagrożenia systemu uczelni wyższej przez cyberatak, jako bardzo niski. Wskazuje na to 389 respondentów, co w udziale procentowym wynosi 77,8% dla kadry administracyjnej i 289 respondentów, co w udziale procentowym dla studentów (różne roczniki) wynosi 57,8%.

Analizując udzielone odpowiedzi w opinii 19 respondentów, co w udziale procentowym wynosi 3,8% dla kadry administracyjnej i 25 respondentów, co w udziale procentowym daje 5% dla studentów studiujących w uczelni wyższej świadczy, że pojawienie się cyberataku stanowi bardzo duże zagrożenie dla systemu informacyjnego uczelni wyższej.

Wykres 3.29. przedstawia odpowiedzi respondentów grupy kadry administracyjnej i grupy studentów (różnych kierunków) na temat stopnia zagrożenia systemu uczelni wyższej przez cyberatak.

Wykres 3.29. Odpowiedzi respondentów grupy kadra administracyjna i grupy studenci (różne kierunki) na temat stopnia zagrożenia systemu uczelni wyższej przez cyberatak



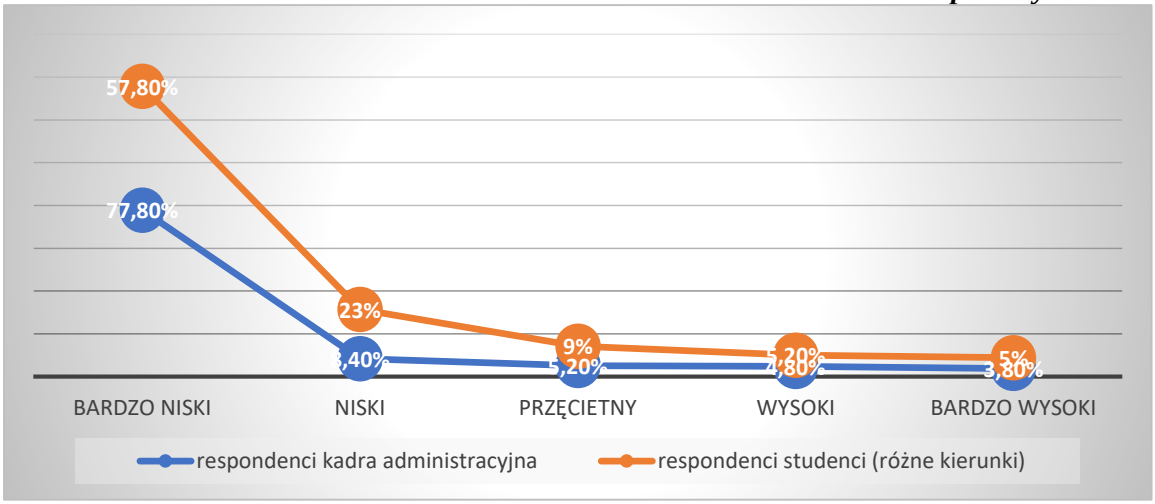
Źródło: opracowanie własne na podstawie badań własnych

O stopniu zależności świadczy współczynnik korelacji liniowej Pearsona na poziomie 0,96 i współczynnik determinacji liniowej, który wskazuje procent wyjaśnionej liniowo zmienności równy 92,16%. Wykres 3.30. pokazuje zależność między respondentami grupy kadra administracyjna i grupy studenci (różne kierunki) pod względem stopnia zagrożenia systemu uczelni wyższej przez cyberatak.

$$r_{xy} = \frac{\frac{1}{n}\sum_{i=1}^{n}(x_i-\bar{x})(y_i-\bar{y})}{S_x S_y}=0{,}96$$

$$WD=r\frac{2}{xy} * 100\% = 92{,}16\%$$

Wykres 3.30. Zależność między respondentami grupy kadra administracyjna i grupy studenci (różne kierunki) pod względem stopnia zagrożenia systemu uczelni wyższej przez cyberatak



Źródło: opracowanie własne na podstawie badań własnych

W związku z faktem, że wartość liczbowa w ocenie relacji jest dodatnia oznacza to, iż wraz ze wzrostem wartości jednej zmiennej rosną wartości także drugiej.

13. Jak Państwo oceniają zagrożenia systemu informacyjnego w uczelni wyższej?

f) Przekazywanie informacji osobom nieupoważnionym

Rozkład odpowiedzi respondentów grupy nauczyciele akademiccy i grupy kadra administracyjna dotyczący oceny przez użytkowników stopnia zagrożenia systemu w uczelni wyższej przez przekazywanie informacji osobom nieuprawnionym zaprezentowano w tabeli 3.16.

Tabela 3.16. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy kadra administracyjna na temat zagrożeń systemu informacyjnego w uczelni wyższej przez przekazywanie informacji osobom nieuprawnionym

Odpowiedzi badanych osób przekazywanie informacji osobom nieuprawnionym						
Osoby poddane badaniu	**Respondenci nauczyciele akademiccy**		**Respondenci kadra administracyjna**		**OGÓŁEM**	
Ocena	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***
bardzo niska	429	85,8%	435	87%	864	86,4%
niska	36	7,2%	28	5,6%	64	6,4%

przeciętna	18	3,6%	17	3,4%	35	3,5%
wysoka	15	3%	15	3%	30	3%
bardzo wysoka	2	0,4%	5	1%	7	0,7%
	500	**100%**	**500**	**100%**	**1000**	**100%**

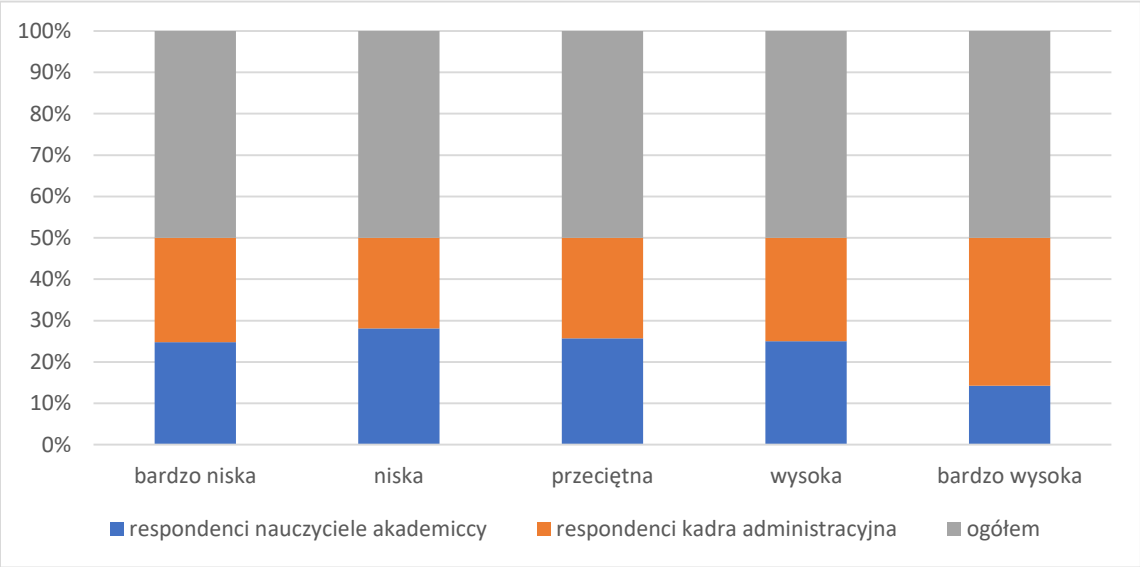
Źródło: opracowanie własne na podstawie badań własnych

W badaniu wzięło udział 500 osób zatrudnionych na stanowisku, nauczycieli akademickich oraz 500 osób zatrudnionych na stanowisku kadra administracyjna. Z przeprowadzonej analizy wynika, że nauczyciele akademiccy jak i kadra administracyjna ocenili stopień zagrożenia systemu uczelni wyższej przez przekazywanie informacji osobom nieuprawnionym, jako bardzo niski. Wskazuje na to 429 respondentów, co w udziale procentowym wynosi 85,8% dla nauczycieli akademickich i 435 respondentów, co w udziale procentowym dla kadry administracyjnej wynosi 87%.

Analizując udzielone odpowiedzi w opinii 2 respondentów, co w udziale procentowym wynosi 0,4% dla nauczycieli akademickich i 5 respondentów, co w udziale procentowym daje 1% dla kadry administracyjnej świadczy, że pojawienie się przekazywania informacji osobom nieupoważnionym stanowi bardzo duże zagrożenie dla systemu informacyjnego uczelni wyższej.

Wykres 3.31. przedstawia odpowiedzi respondentów grupy nauczyciele akademiccy i grupy kadra administracyjna na temat stopnia zagrożenia systemu uczelni wyższej przez przekazywanie informacji osobom nieuprawnionym.

Wykres 3.31. Odpowiedzi respondentów grupy nauczyciele akademiccy i kadry administracyjnej na temat stopnia zagrożenia systemu uczelni wyższej przez przekazywanie informacji osobom nieuprawnionym



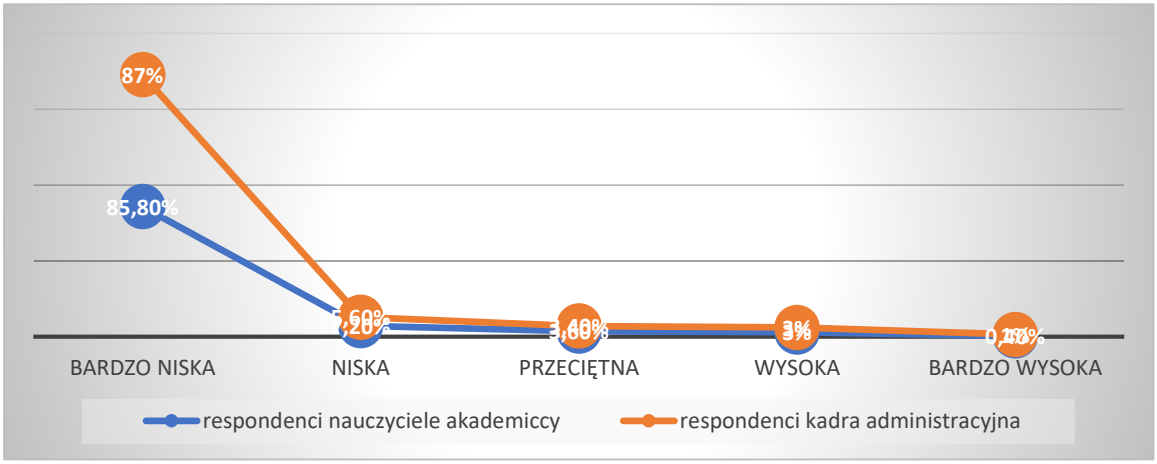
Źródło: opracowanie własne na podstawie badań własnych

O stopniu zależności świadczy współczynnik korelacji liniowej Pearsona na poziomie 1 i współczynnik determinacji liniowej, który wskazuje procent wyjaśnionej liniowo zmienności równy 100%. Wykres 3.32. pokazuje zależność między respondentami grupy nauczyciele akademiccy i grupy kadra administracyjna pod względem stopnia zagrożenia systemu uczelni wyższej przez przekazywanie informacji osobom nieuprawnionym.

$$r_{xy} = \frac{\frac{1}{n}\sum_{i=1}^{n}(x_i-\bar{x})(y_i-\bar{y})}{S_x S_y}=1$$

$$\mathrm{WD}=r\frac{2}{xy} * 100\% = 100\%$$

Wykres 3.32. Zależność między respondentami grupy nauczyciele akademiccy i grupy kadra administracyjna pod względem stopnia zagrożenia systemu uczelni wyższej przez przekazywanie informacji osobom nieuprawnionym



Źródło: opracowanie własne na podstawie badań własnych

W związku z faktem, że wartość liczbowa w ocenie relacji jest dodatnia oznacza to, iż wraz ze wzrostem wartości jednej zmiennej rosną wartości także drugiej. Tabela 3.17. przedstawia odpowiedzi respondentów grupy nauczyciele akademiccy i grupy studenci (różne kierunki) na temat zagrożeń systemu informacyjnego w uczelni wyższej przez przekazywanie informacji osobom nieuprawnionym.

Tabela 3.17. ***Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy studenci (różne kierunki) na temat zagrożeń systemu informacyjnego w uczelni wyższej przez przekazywanie informacji osobom nieuprawnionym***

Odpowiedzi badanych osób przekazywanie informacji osobom nieuprawnionym						
Osoby poddane badaniu	**Respondenci nauczyciele akademiccy**		**Respondenci studenci (różne kierunki)**		**OGÓŁEM**	
Ocena	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***
bardzo niska	429	85,8%	298	59,6%	727	72,7%
niska	36	7,2%	168	33,6%	204	20,4%
przeciętna	18	3,6%	12	2,4%	30	3%
wysoka	15	3%	13	2,6%	28	2,8%
bardzo wysoka	2	0,4%	9	1,8%	11	1,1%
	500	**100%**	**500**	**100%**	**1000**	**100%**

Źródło: opracowanie własne na podstawie badań własnych

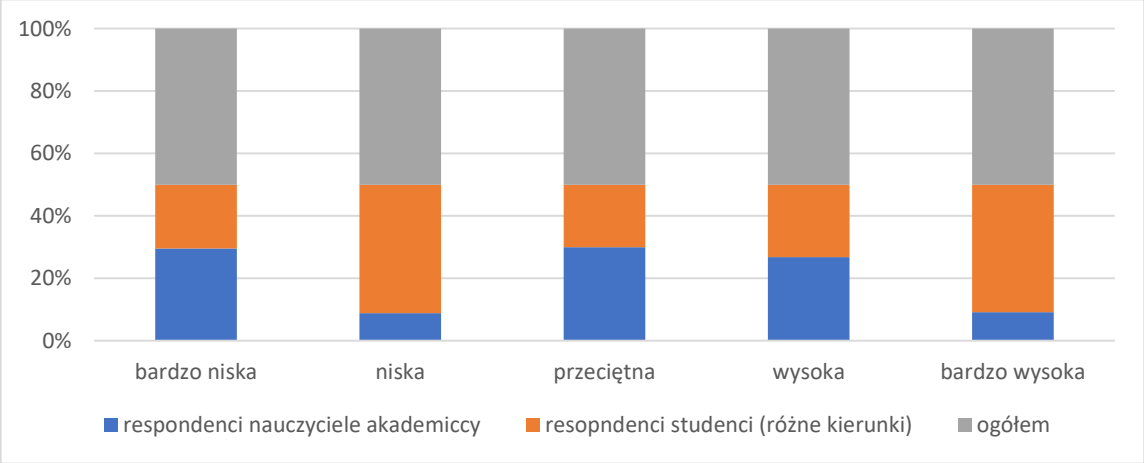
W badaniu wzięło udział 500 osób zatrudnionych na stanowisku, nauczycieli akademickich oraz 500 osób studiujących w uczelni wyższej. Z przeprowadzonej analizy

wynika, że nauczyciele akademiccy jak i studenci (różne kierunki) ocenili stopień zagrożenia systemu uczelni wyższej przez przekazywanie informacji osobom nieuprawnionym, jako bardzo niski. Wskazuje na to 429 respondentów, co w udziale procentowym wynosi 85,8% dla nauczycieli akademickich i 298 respondentów, co w udziale procentowym dla studentów (różne roczniki) wynosi 59,6%.

Analizując udzielone odpowiedzi w opinii 2 respondentów, co w udziale procentowym wynosi 0,4% dla nauczycieli akademickich i 9 respondentów, co w udziale procentowym daje 1,8% dla studentów studiujących w uczelni wyższej świadczy, że pojawienie się przekazywania informacji osobom nieuprawnionym stanowi bardzo duże zagrożenie dla systemu informacyjnego uczelni wyższej.

Wykres 3.33. przedstawia odpowiedzi respondentów grupy nauczyciele akademiccy i grupy studenci (różne kierunki) na temat stopnia zagrożenia systemu uczelni wyższej przez przekazywanie informacji osobom nieuprawnionym.

Wykres 3.33. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy studenci (różne kierunki) na temat stopnia zagrożenia systemu uczelni wyższej przez przekazywanie informacji osobom nieuprawnionym



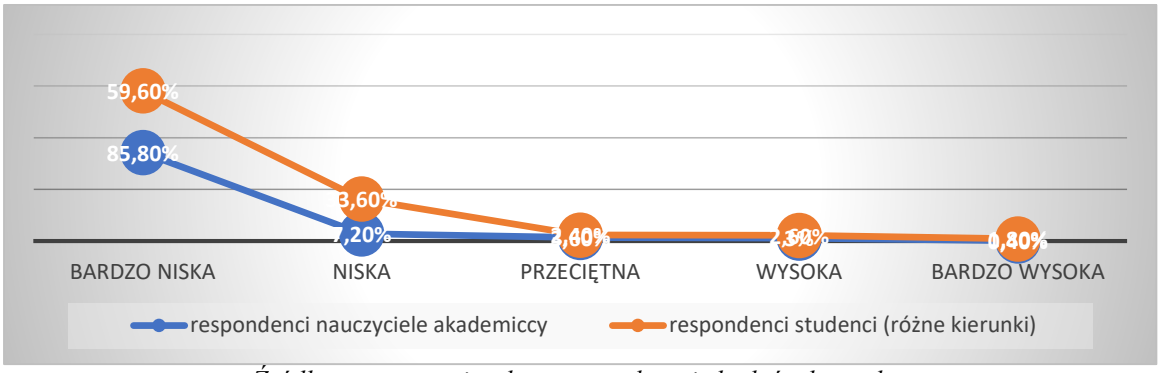
Źródło: opracowanie własne na podstawie badań własnych

O stopniu zależności świadczy współczynnik korelacji liniowej Pearsona na poziomie 0,88 i współczynnik determinacji liniowej, który wskazuje procent wyjaśnionej liniowo zmienności równy 77,44%. Wykres 3.34. pokazuje zależność między respondentami grupy nauczyciele akademiccy i grupy studenci (różne kierunki) pod względem stopnia zagrożenia systemu uczelni wyższej przez przekazywanie informacji osobom nieuprawnionym.

$$r_{xy} = \frac{\frac{1}{n}\sum_{i=1}^{n}(x_i-\bar{x})(y_i-\bar{y})}{S_x S_y}=0{,}88$$

$$\mathrm{WD}=r_{xy}^{2} * 100\% = 77{,}44\%$$

Wykres 3.34. Zależność między respondentami grupy nauczyciele akademiccy i grupy studenci (różne kierunki) pod względem stopnia zagrożenia systemu uczelni wyższej przez przekazywanie informacji osobom nieuprawnionym



Źródło: opracowanie własne na podstawie badań własnych

W związku z faktem, że wartość liczbowa w ocenie relacji jest dodatnia oznacza to, iż wraz ze wzrostem wartości jednej zmiennej rosną wartości także drugiej. Tabela 3.18. przedstawia odpowiedzi respondentów grupy nauczyciele akademiccy i grupy studenci (różne kierunki) na temat zagrożeń systemu informacyjnego w uczelni wyższej przez przekazywanie informacji osobom nieuprawnionym.

Tabela 3.18. Odpowiedzi respondentów grupy kadra administracyjna i grupy studenci (różne kierunki) na temat zagrożeń systemu informacyjnego w uczelni wyższej przez przekazywanie informacji osobom nieuprawnionym

Odpowiedzi badanych osób przekazywanie informacji osobom nieuprawnionym						
Osoby poddane badaniu	**Respondenci kadra administracyjna**		**Respondenci studenci (różne kierunki)**		**OGÓŁEM**	
Ocena	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***
bardzo niska	435	87%	298	59,6%	733	73,3%
niska	28	5,6%	168	33,6%	196	19,6%
przeciętna	17	3,4%	12	2,4%	29	2,9%
wysoka	15	3%	13	2,6%	28	2,8%
bardzo wysoka	5	1%	9	1,8%	14	1,4%
	500	**100%**	**500**	**100%**	**1000**	**100%**

Źródło: opracowanie własne na podstawie badań własnych

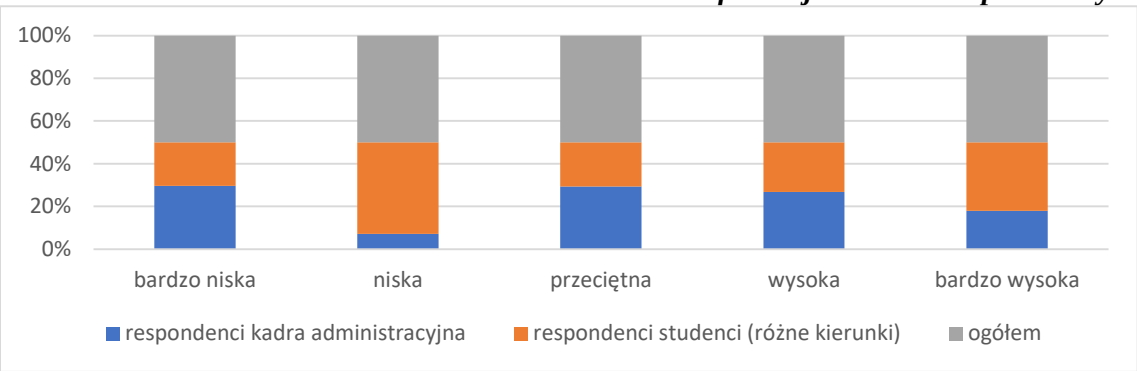
W badaniu wzięło udział 500 osób zatrudnionych na stanowisku, kadra administracyjna oraz 500 osób studiujących w uczelni wyższej. Z przeprowadzonej analizy wynika, że kadra administracyjna jak i studenci (różne kierunki) ocenili stopień zagrożenia

systemu uczelni wyższej przez przekazywanie informacji osobom nieuprawnionym, jako bardzo niski. Wskazuje na to 435 respondentów, co w udziale procentowym wynosi 87% kadry administracyjnej i 298 respondentów, co w udziale procentowym dla studentów (różne roczniki) wynosi 59,6%.

Analizując udzielone odpowiedzi w opinii 5 respondentów, co w udziale procentowym wynosi 1% dla kadry administracyjnej i 9 respondentów, co w udziale procentowym daje 1,8% dla studentów studiujących w uczelni wyższej świadczy, że pojawienie się przekazywania informacji osobom nieuprawnionym stanowi bardzo duże zagrożenie dla systemu informacyjnego uczelni wyższej.

Wykres 3.35. przedstawia odpowiedzi respondentów grupy kadra administracyjna i grupy studenci (różne kierunki) na temat stopnia zagrożenia systemu uczelni wyższej przez przekazywanie informacji osobom nieuprawnionym.

Wykres 3.35. Odpowiedzi respondentów grupy kadra administracyjna i grupy studenci (różne kierunki) na temat stopnia zagrożenia systemu uczelni wyższej przez przekazywanie informacji osobom nieuprawnionym



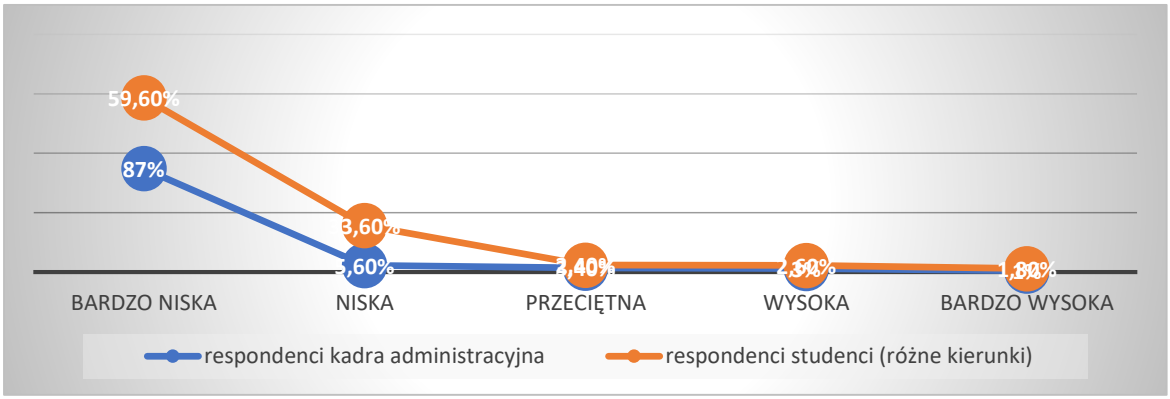
Źródło: opracowanie własne na podstawie badań własnych

O stopniu zależności świadczy współczynnik korelacji liniowej Pearsona na poziomie 0,87 i współczynnik determinacji liniowej, który wskazuje procent wyjaśnionej liniowo zmienności równy 75,69%. Wykres 3.36. pokazuje zależność między respondentami grupy kadra administracyjna grupy studenci (różne kierunki) pod względem stopnia zagrożenia systemu uczelni wyższej przez przekazywanie informacji osobom nieuprawnionym.

$$r_{xy} = \frac{\frac{1}{n}\sum_{i=1}^{n}(x_i-\bar{x})(y_i-\bar{y})}{S_x S_y}=0{,}87$$

$$\mathrm{WD}=r_{xy}^{2} * 100\% = 75{,}69\%$$

Wykres 3.36. Zależność między respondentami grupy kadra administracyjna i grupy studenci (różne kierunki) pod względem stopnia zagrożenia systemu uczelni wyższej przez przekazywanie informacji osobom nieuprawnionym



Źródło: opracowanie własne na podstawie badań własnych

W związku z faktem, że wartość liczbowa w ocenie relacji jest dodatnia oznacza to, iż wraz ze wzrostem wartości jednej zmiennej rosną wartości także drugiej.

13. Jak Państwo oceniają zagrożenia systemu informacyjnego w uczelni wyższej?

g) Celowe pozorowanie awarii systemu

Rozkład odpowiedzi respondentów grupy nauczyciele akademiccy i kadra administracyjna dotyczący oceny przez użytkowników stopnia zagrożenia systemu uczelni wyższej przez celowe pozorowanie awarii systemu prezentuje tabela 3.19.

Tabela 3.19. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy kadra administracyjna na temat zagrożeń systemu informacyjnego w uczelni wyższej przez celowe pozorowanie awarii systemu

Odpowiedzi badanych osób celowe pozorowanie awarii systemu						
Osoby poddane badaniu	**Respondenci nauczyciele akademiccy**		**Respondenci kadra administracyjna**		**OGÓŁEM**	
Ocena	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***
bardzo niska	437	87,4%	443	88,6%	880	88%
niska	38	7,6%	19	3,8%	57	5,7%
przeciętna	15	3%	15	3%	30	3%
wysoka	8	1,6%	16	3,2%	24	2,4%
bardzo wysoka	2	0,4%	7	1,4%	9	0,9%
	500	**100%**	**500**	**100%**	**1000**	**100%**

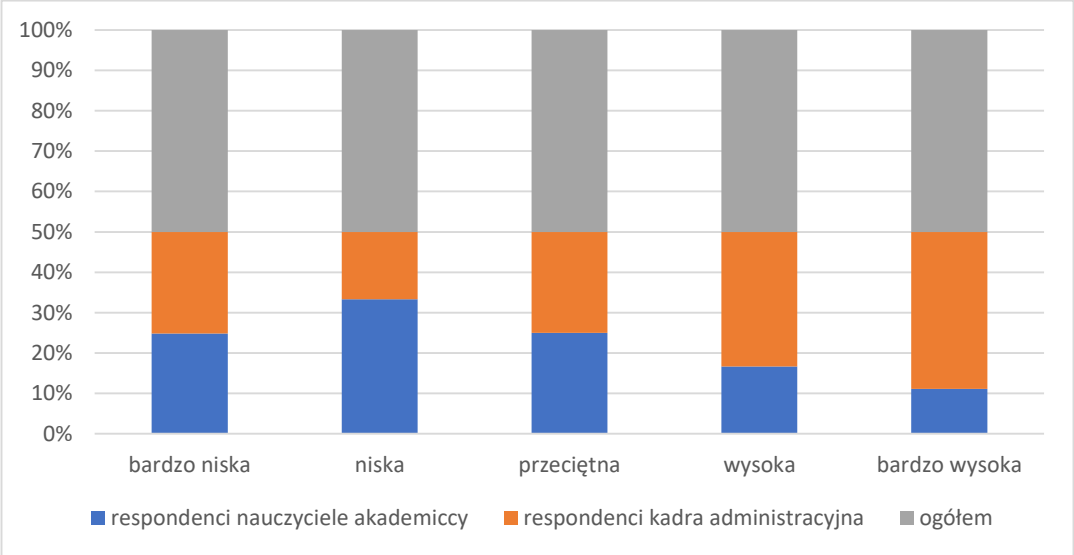
Źródło: opracowanie własne na podstawie badań własnych

W badaniu wzięło udział 500 osób zatrudnionych na stanowisku, nauczycieli akademickich oraz 500 osób zatrudnionych na stanowisku kadra administracyjna. Z przeprowadzonej analizy wynika, że nauczyciele akademiccy jak i kadra administracyjna ocenili stopień zagrożenia systemu uczelni wyższej przez celowe pozorowanie awarii systemu, jako bardzo niski. Wskazuje na to 427 respondentów, co w udziale procentowym wynosi 87,4% dla nauczycieli akademickich i 443 respondentów, co w udziale procentowym dla kadry administracyjnej wynosi 88,6%.

Analizując udzielone odpowiedzi w opinii 2 respondentów, co w udziale procentowym wynosi 0,4% dla nauczycieli akademickich i 7 respondentów, co w udziale procentowym daje 1,44% dla kadry administracyjnej świadczy, że pojawienie się celowo pozorowanych awarii systemu stanowi bardzo duże zagrożenie dla systemu informacyjnego uczelni wyższej.

Wykres 3.37. przedstawia odpowiedzi respondentów grupy nauczyciele akademiccy i grupy kadra administracyjna na temat stopnia zagrożenia systemu uczelni wyższej przez celowe pozorowanie awarii systemu.

Wykres 3.37. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy kadra administracyjna na temat stopnia zagrożenia systemu uczelni wyższej przez celowe pozorowanie awarii systemu



Źródło: opracowanie własne na podstawie badań własnych

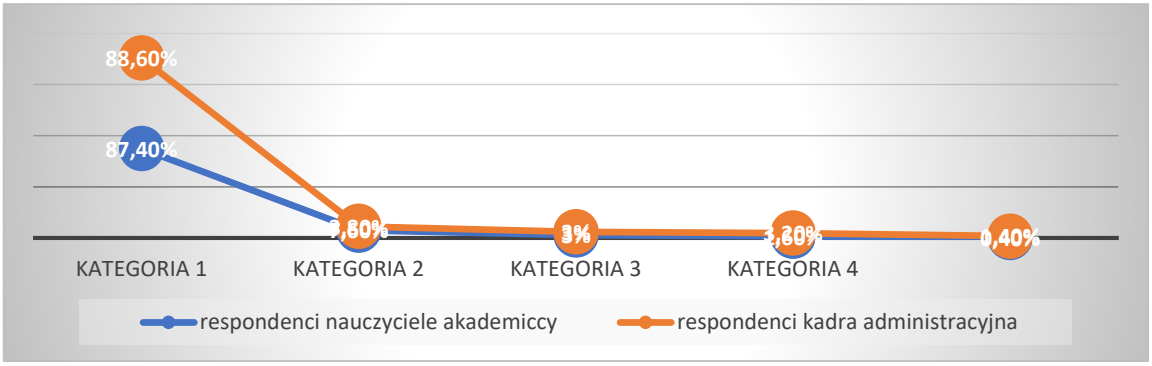
O stopniu zależności świadczy współczynnik korelacji liniowej Pearsona na poziomie 0,99 i współczynnik determinacji liniowej, który wskazuje procent wyjaśnionej

liniowo zmienności równy 98,01%. Wykres 3.38. pokazuje zależność między respondentami grupy nauczyciele akademiccy i grupy kadra administracyjna pod względem stopnia zagrożenia systemu uczelni wyższej przez celowe pozorowanie awarii systemu.

$$r_{xy} = \frac{\frac{1}{n}\sum_{i=1}^{n}(x_i-\bar{x})(y_i-\bar{y})}{S_x S_y}=0{,}99$$

$$\mathrm{WD}=r_{xy}^{2} * 100\% = 98{,}01\%$$

Wykres 3.38. Zależność między respondentami grupy nauczyciele akademiccy i grupy kadra administracyjna pod względem stopnia zagrożenia systemu uczelni wyższej przez celowe pozorowanie awarii systemu



Źródło: opracowanie własne na podstawie badań własnych

W związku z faktem, że wartość liczbowa w ocenie relacji jest dodatnia oznacza to, iż wraz ze wzrostem wartości jednej zmiennej rosną wartości także drugiej. Tabela 3.20. przedstawia odpowiedzi respondentów grupy nauczyciele akademiccy i grupy studenci (różne kierunki) na temat zagrożeń systemu informacyjnego w uczelni wyższej przez celowe pozorowanie awarii systemu.

Tabela 3.20. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy studenci (różne kierunki) na temat zagrożeń systemu informacyjnego w uczelni wyższej przez celowe pozorowanie awarii systemu

Odpowiedzi badanych osób celowe pozorowanie awarii systemu						
Osoby poddane badaniu	**Respondenci nauczyciele akademiccy**		**Respondenci studenci (różne kierunki)**		**OGÓŁEM**	
Ocena	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***
bardzo niska	437	87,4%	276	55,2%	713	71,3%
niska	38	7,6%	189	37,8%	227	22,7%
przeciętna	15	3%	16	3,2%	31	3,1%
wysoka	8	1,6%	15	3%	23	2,3%
bardzo wysoka	2	0,4%	9	1,8%	11	1,1%
	500	**100%**	**500**	**100%**	**1000**	**100%**

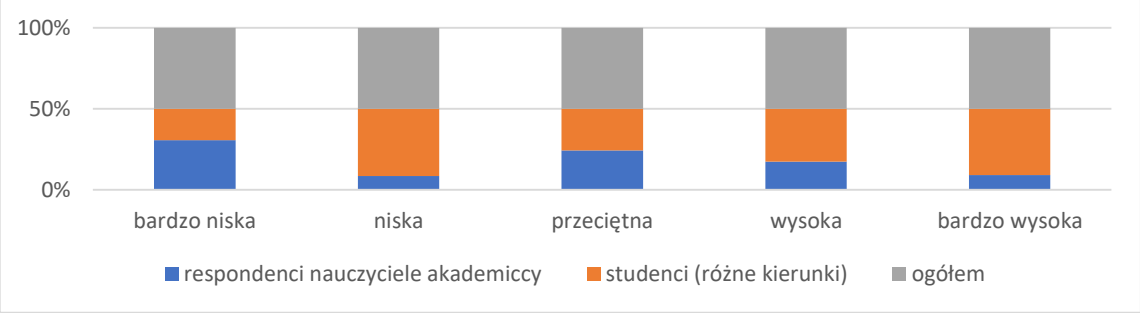
Źródło: opracowanie własne na podstawie badań własnych

W badaniu wzięło udział 500 osób zatrudnionych na stanowisku, nauczycieli akademickich oraz 500 osób studiujących w uczelni wyższej. Z przeprowadzonej analizy wynika, że nauczyciele akademiccy jak i studenci (różne kierunki) ocenili stopień zagrożenia systemu uczelni wyższej przez celowe pozorowanie awarii systemu, jako bardzo niski. Wskazuje na to 437 respondentów, co w udziale procentowym wynosi 87,4% dla nauczycieli akademickich i 276 respondentów, co w udziale procentowym dla studentów (różne roczniki) wynosi 55,2%.

Analizując udzielone odpowiedzi w opinii 2 respondentów, co w udziale procentowym wynosi 0,4% dla nauczycieli akademickich i 9 respondentów, co w udziale procentowym daje 1,8% dla studentów studiujących w uczelni wyższej świadczy, że pojawienie się celowo pozorowanych awarii systemów stanowi bardzo duże zagrożenie dla systemu informacyjnego uczelni wyższej.

Wykres 3.39. przedstawia odpowiedzi respondentów grupy nauczyciele akademiccy i grupy studenci (różne kierunki) na temat stopnia zagrożenia systemu uczelni wyższej przez celowe pozorowanie awarii systemu.

Wykres 3.39. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy studenci (różne kierunki) na temat stopnia zagrożenia systemu uczelni wyższej przez celowe pozorowanie awarii systemu



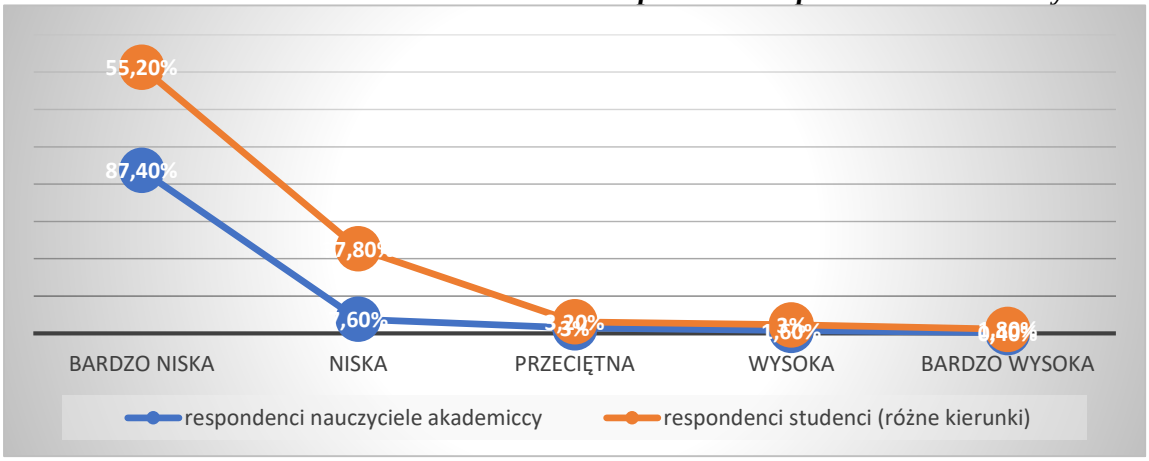
Źródło: opracowanie własne na podstawie badań własnych

O stopniu zależności świadczy współczynnik korelacji liniowej Pearsona na poziomie 0,83 i współczynnik determinacji liniowej, który wskazuje procent wyjaśnionej liniowo zmienności równy 68,89%. Wykres 3.40. pokazuje zależność między respondentami grupy nauczyciele akademiccy i grupy studenci (różne kierunki) pod względem stopnia zagrożenia systemu uczelni wyższej przez celowe pozorowanie awarii systemu.

$$r_{xy} = \frac{\frac{1}{n}\sum_{i=1}^{n}(x_i-\bar{x})(y_i-\bar{y})}{S_x S_y}=0{,}83$$

$$WD=r\frac{2}{xy} * 100\% = 68{,}89\%$$

Wykres 3.40. Zależność między respondentami grupy nauczyciele akademiccy i grupy studenci (różne kierunki) pod względem stopnia zagrożenia systemu uczelni wyższej przez celowe pozorowanie awarii systemu



Źródło: opracowanie własne na podstawie badań własnych

W związku z faktem, że wartość liczbowa w ocenie relacji jest dodatnia oznacza to, iż wraz ze wzrostem wartości jednej zmiennej rosną wartości także drugiej. Tabela 3.21. przedstawia odpowiedzi respondentów grupy kadra administracyjna i grupy studenci (różne kierunki) na temat zagrożeń systemu informacyjnego w uczelni wyższej przez celowe pozorowanie awarii systemu.

Tabela 48 Tabela 3.21. Odpowiedzi respondentów grupy kadra administracyjna i grupy studenci (różne kierunki) na temat zagrożeń systemu informacyjnego w uczelni wyższej przez celowe pozorowanie awarii systemu

Odpowiedzi badanych osób celowe pozorowanie awarii systemu						
Osoby poddane badaniu	**Respondenci kadra administracyjna**		**Respondenci studenci (różne kierunki)**		**OGÓŁEM**	
Ocena	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***
bardzo niska	443	88,6%	276	55,2%	719	71,9%
niska	19	3,8%	189	37,8%	208	20,8%
przeciętna	15	3%	16	3,2%	31	3,1%
wysoka	16	3,2%	15	3%	31	3,1%
bardzo wysoka	7	1,4%	9	1,8%	16	1,6%

Źródło: opracowanie własne na podstawie badań własnych

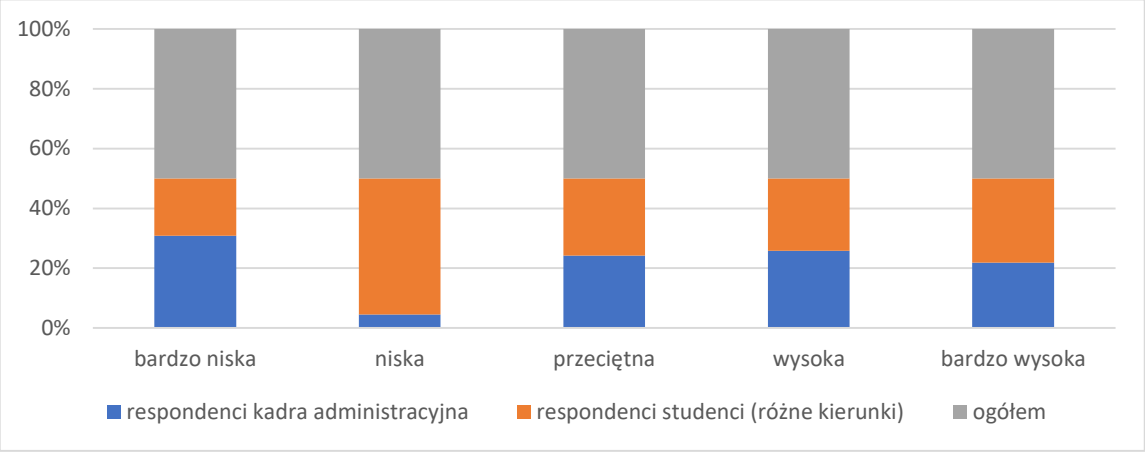
W badaniu wzięło udział 500 osób zatrudnionych na stanowisku, kadra administracyjna oraz 500 osób studiujących w uczelni wyższej. Z przeprowadzonej analizy wynika, że kadra administracyjna jak i studenci (różne kierunki) ocenili stopień zagrożenia systemu uczelni wyższej przez celowe pozorowanie awarii systemu, jako bardzo niski.

Wskazuje na to 443 respondentów, co w udziale procentowym wynosi 55,2% dla kadry administracyjnej i 276 respondentów, co w udziale procentowym dla studentów (różne roczniki) wynosi 55,2%.

Analizując udzielone odpowiedzi w opinii 7 respondentów, co w udziale procentowym wynosi 1,4% dla kadry administracyjnej i 9 respondentów, co w udziale procentowym daje 1,8% dla studentów studiujących w uczelni wyższej świadczy, że pojawienie się celowych pozorowanych awarii systemu stanowi bardzo duże zagrożenie dla systemu informacyjnego uczelni wyższej.

Wykres 3.41. przedstawia odpowiedzi respondentów grupy kadra administracyjna i grupy studenci (różne kierunki) na temat stopnia zagrożenia systemu uczelni wyższej przez celowe pozorowanie awarii systemu.

Wykres 3.41. Odpowiedzi respondentów grupy kadra administracyjna grupy studenci (różne kierunki) na temat stopnia zagrożenia systemu uczelni wyższej przez celowe pozorowanie awarii systemu



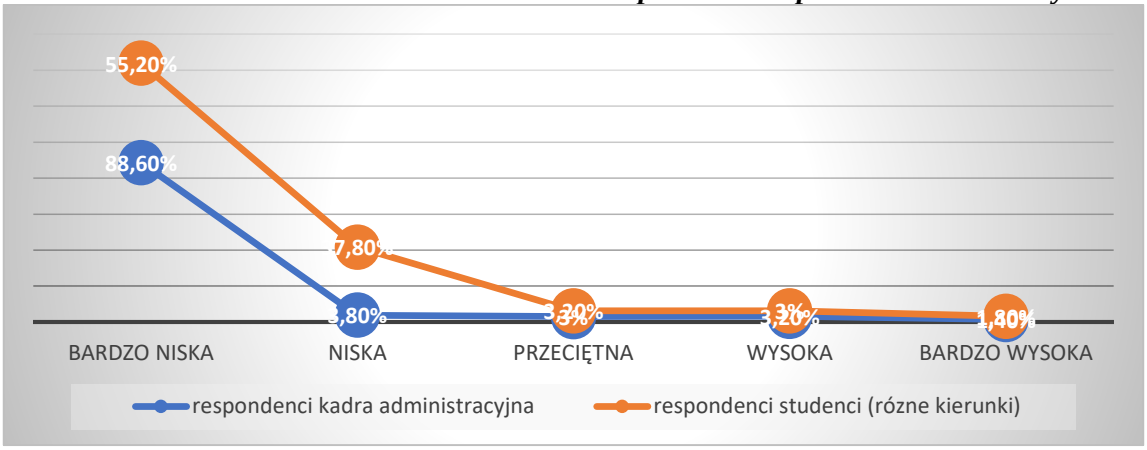
Źródło: opracowanie własne na podstawie badań własnych

O stopniu zależności świadczy współczynnik korelacji liniowej Pearsona na poziomie 0,80 i współczynnik determinacji liniowej, który wskazuje procent wyjaśnionej liniowo zmienności równy 64%. Wykres 3.42. pokazuje zależność między respondentami grupy kadra administracyjna i grupy studenci (różne kierunki) pod względem stopnia zagrożenia systemu uczelni wyższej przez celowe pozorowanie awarii systemu.

$$r_{xy} = \frac{\frac{1}{n}\sum_{i=1}^{n}(x_i-\bar{x})(y_i-\bar{y})}{S_x S_y}=0{,}80$$

$$\mathrm{WD}=r_{xy}^{2} * 100\% = 64\%$$

Wykres 3.42. Zależność między respondentami grupy kadra administracyjna i grupy studenci (różne kierunki) pod względem stopnia zagrożenia systemu uczelni wyższej przez celowe pozorowanie awarii systemu



Źródło: opracowanie własne na podstawie badań własnych

W związku z faktem, że wartość liczbowa w ocenie relacji jest dodatnia oznacza to, iż wraz ze wzrostem wartości jednej zmiennej rosną wartości także drugiej.

13. Jak Państwo oceniają zagrożenia systemu informacyjnego w uczelni wyższej?

h) Wykorzystywanie luk w zabezpieczeniach dostępu do poczty elektronicznej i serwisu informacyjnego

Rozkład odpowiedzi respondentów grupy nauczycieli akademickich i grupy kadry administracyjnej dotyczący oceny przez użytkowników stopnia zagrożenia systemu uczelni wyższej przez wykorzystanie luk w zabezpieczeniach dostępu do poczty elektronicznej i serwisu informacyjnego prezentuje tabela 3.22.

Tabela 3.22. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy kadra administracyjna na temat zagrożeń systemu informacyjnego w uczelni wyższej przez wykorzystywanie luk w zabezpieczeniach dostępu do poczty elektronicznej i serwisu informacyjnego

Odpowiedzi badanych osób wykorzystywanie luk w zabezpieczeniach dostępu do poczty elektronicznej i serwisu informacyjnego						
Osoby poddane badaniu	**Respondenci nauczyciele akademiccy**		**Respondenci kadra administracyjna**		**OGÓŁEM**	
Ocena	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***
bardzo niska	16	3,2%	259	51,8%	275	27,5%
niska	423	84,6%	169	33,8%	592	59,2%
przeciętna	28	5,6%	46	9,2%	74	7,4%
wysoka	19	3,8%	23	4,6%	42	4,2%
bardzo wysoka	14	2,8%	3	3%	17	1,7%
	500	**100%**	**500**	**100%**	**1000**	**100%**

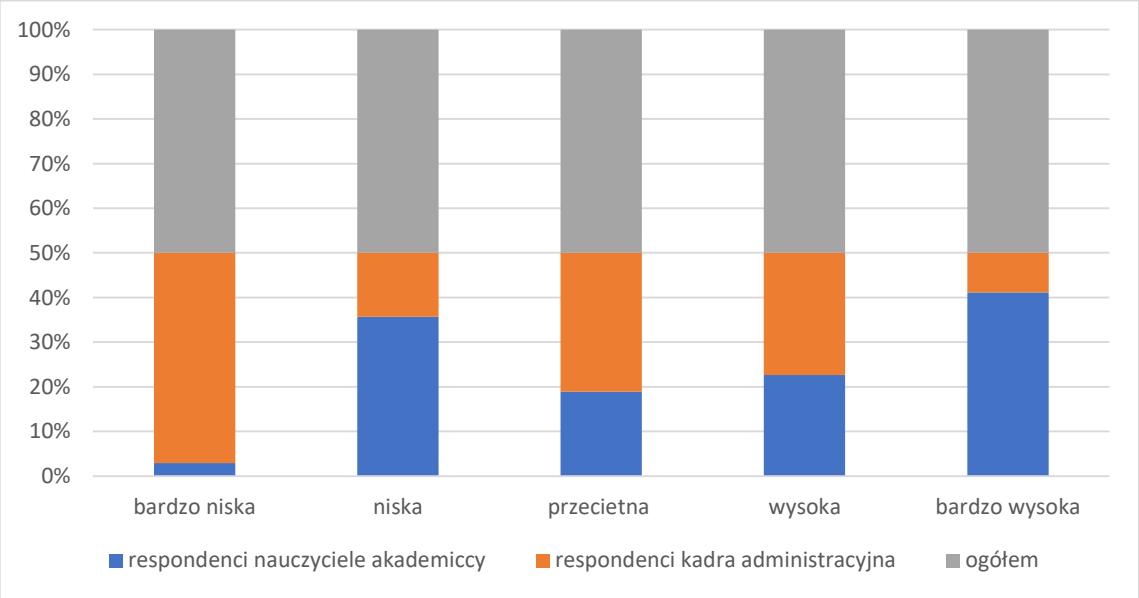
Źródło: opracowanie własne na podstawie badań własnych

W badaniu wzięło udział 500 osób zatrudnionych na stanowisku, nauczycieli akademickich oraz 500 osób zatrudnionych na stanowisku kadry administracyjnej. Z przeprowadzonej analizy wynika, że nauczyciele akademiccy jak i kadra administracyjna ocenili stopień zagrożenia systemu uczelni wyższej przez wykorzystanie luk w zabezpieczeniach do poczty elektronicznej i serwisu informacyjnego, jako niski i bardzo niski. Wskazuje na to 423 respondentów, co w udziale procentowym wynosi 84,6% dla nauczycieli akademickich i 259 respondentów, co w udziale procentowym dla kadry administracyjnej wynosi 51,8%.

Analizując udzielone odpowiedzi w opinii 14 respondentów, co w udziale procentowym wynosi 2,8% dla nauczycieli akademickich i 3 respondentów, co w udziale procentowym daje 3% dla kadry administracyjnej świadczy, że pojawienie się wykorzystania luk w zabezpieczeniach do poczty elektronicznej i serwisu informacyjnego stanowi bardzo duże zagrożenie dla systemu informacyjnego uczelni wyższej.

Wykres 3.43. przedstawia odpowiedzi respondentów grupy nauczyciele akademiccy i grupy kadra administracyjna na temat stopnia zagrożenia systemu uczelni wyższej przez wykorzystanie luk w zabezpieczeniach do poczty elektronicznej i serwisu informacyjnego.

Wykres 3.43. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy kadra administracyjna na temat stopnia zagrożenia systemu uczelni wyższej przez wykorzystanie luk w zabezpieczeniach do poczty elektronicznej i serwisu informacyjnego



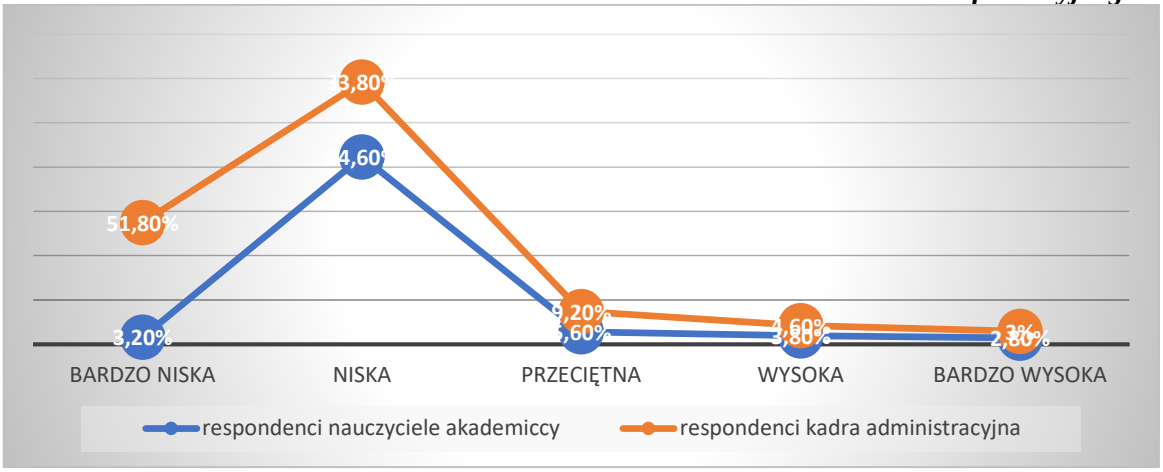
Źródło: opracowanie własne na podstawie badań własnych

O stopniu zależności świadczy współczynnik korelacji liniowej Pearsona na poziomie 0,34 i współczynnik determinacji liniowej, który wskazuje procent wyjaśnionej liniowo zmienności równy 11,56%. Wykres 3.44. pokazuje zależność między respondentami grupy nauczyciele akademiccy i grupy kadra administracyjna pod względem stopnia zagrożenia systemu uczelni wyższej przez wykorzystanie luk w zabezpieczeniach do poczty elektronicznej i serwisu informacyjnego.

$$r_{xy} = \frac{\frac{1}{n}\sum_{i=1}^{n}(x_i-\bar{x})(y_i-\bar{y})}{S_x S_y}=0{,}34$$

$$\text{WD}=r_{xy}^{2} * 100\% = 11{,}56\%$$

Wykres 3.44. Zależność między respondentami grupy nauczyciele akademiccy i grupy studenci (różne kierunki) pod względem stopnia zagrożenia systemu uczelni wyższej przez wykorzystanie luk w zabezpieczeniach do poczty elektronicznej i serwisu informacyjnego



Źródło: opracowanie własne na podstawie badań własnych

W związku z faktem, że wartość liczbowa w ocenie relacji jest dodatnia oznacza to, iż wraz ze wzrostem wartości jednej zmiennej rosną wartości także drugiej. Tabela 3.23. przedstawia odpowiedzi respondentów grupy nauczyciele akademiccy i grupy studenci (różne kierunki) na temat zagrożeń systemu informacyjnego w uczelni wyższej przez wykorzystanie luk w zabezpieczeniach do poczty elektronicznej i serwisu informacyjnego.

Tabela 3.23. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy studenci (różne kierunki) na temat zagrożeń systemu informacyjnego w uczelni wyższej przez wykorzystanie luk w zabezpieczeniach do poczty elektronicznej i serwisu informacyjnego

Odpowiedzi badanych osób wykorzystywanie luk w zabezpieczeniach dostępu do poczty elektronicznej i serwisu informacyjnego			
Osoby poddane badaniu	**Respondenci nauczyciele akademiccy**	**Respondenci studenci (różne kierunki)**	**OGÓŁEM**

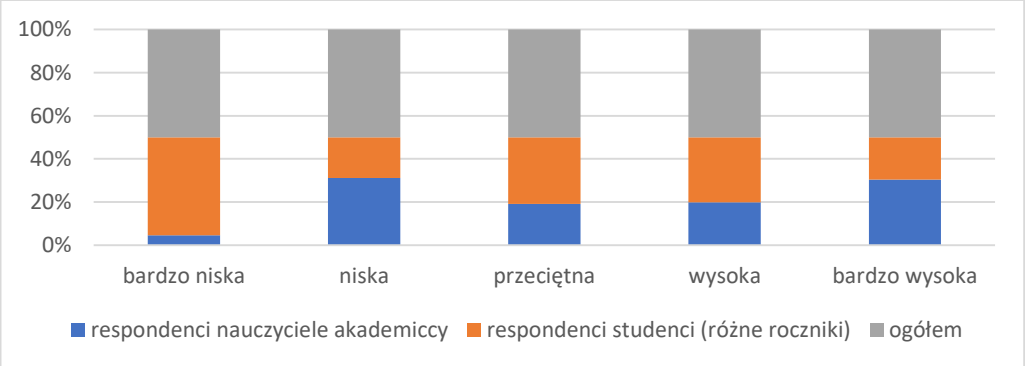
Ocena	*liczba wskazań*	*udział procentowy*	*liczba wskazań*	*udział procentowy*	*liczba wskazań*	*udział procentowy*
bardzo niska	16	3,2%	162	32,4%	178	17,8%
niska	423	84,6%	255	51%	678	67,8%
przeciętna	28	5,6%	45	9%	73	7,3%
wysoka	19	3,8%	29	5,8%	48	4,8%
bardzo wysoka	14	2,8%	9	1,8%	23	2,3%
	500	**100%**	**500**	**100%**	**1000**	**100%**

Źródło: opracowanie własne na podstawie badań własnych

W badaniu wzięło udział 500 osób zatrudnionych na stanowisku, nauczycieli akademickich oraz 500 osób studiujących w uczelni wyższej. Z przeprowadzonej analizy wynika, że nauczyciele akademiccy jak i studenci (różne kierunki) ocenili stopień zagrożenia systemu uczelni wyższej przez wykorzystanie luk w zabezpieczeniach do poczty elektronicznej i serwisu informacyjnego niski. Wskazuje na to 423 respondentów, co w udziale procentowym wynosi 84,6% dla nauczycieli akademickich i 255 respondentów, co w udziale procentowym dla studentów (różne roczniki) wynosi 51%.

Analizując udzielone odpowiedzi w opinii 14 respondentów, co w udziale procentowym wynosi 2,8% dla nauczycieli akademickich i 9 respondentów, co w udziale procentowym daje 1,8% dla studentów studiujących w uczelni wyższej świadczy, że pojawienie się wykorzystania luk w zabezpieczeniach do poczty elektronicznej i serwisu informacyjnego stanowi bardzo duże zagrożenie dla systemu informacyjnego uczelni wyższej. Wykres 3.45. przedstawia odpowiedzi respondentów grupy nauczyciele akademiccy i grupy studenci (różne roczniki) na temat stopnia zagrożenia systemu uczelni wyższej przez wykorzystanie luk w zabezpieczeniach do poczty elektronicznej i serwisu informacyjnego.

Wykres 3.45. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy studenci (różne kierunki) na temat stopnia zagrożenia systemu uczelni wyższej przez wykorzystanie luk w zabezpieczeniach do poczty elektronicznej i serwisu informacyjnego



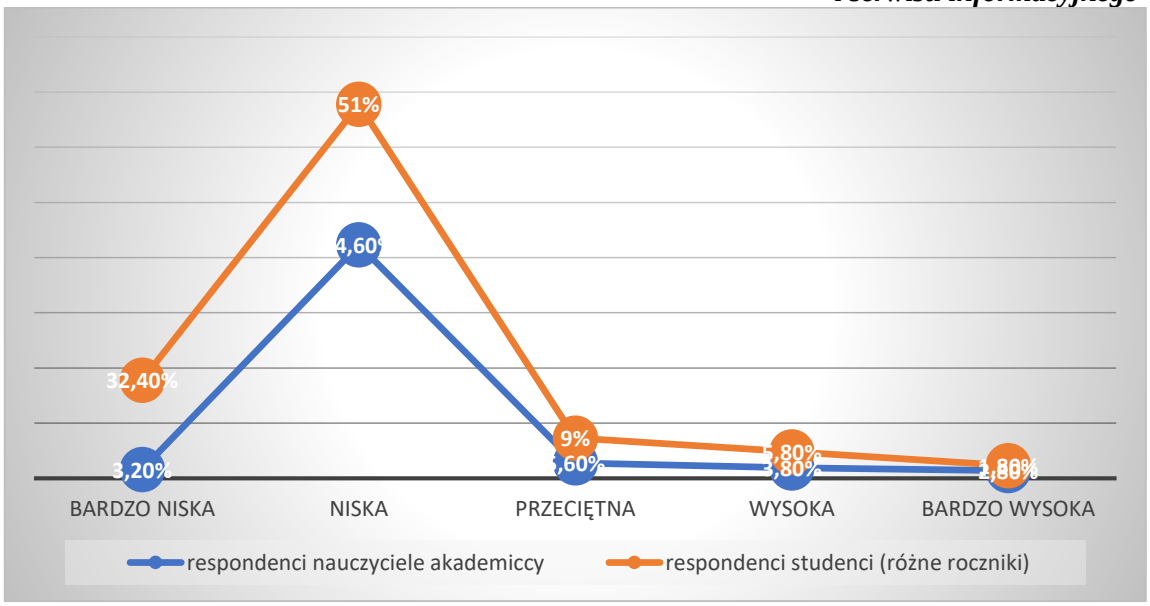
Źródło: opracowanie własne na podstawie badań własnych

O stopniu zależności świadczy współczynnik korelacji liniowej Pearsona na poziomie 0,82 i współczynnik determinacji liniowej, który wskazuje procent wyjaśnionej liniowo zmienności równy 67,24%. Wykres 3.46. pokazuje zależność między respondentami grupy nauczyciele akademiccy i grupy studenci (różne roczniki) pod względem stopnia zagrożenia systemu uczelni wyższej przez wykorzystanie luk w zabezpieczeniach do poczty elektronicznej i serwisu informacyjnego.

$$r_{xy} = \frac{\frac{1}{n}\sum_{i=1}^{n}(x_i-\bar{x})(y_i-\bar{y})}{S_x S_y}=0{,}82$$

$$\mathrm{WD}=r_{xy}^{2} * 100\% = 67{,}24\%$$

Wykres 3.46. Zależność między respondentami grupy nauczyciele akademiccy i grupy studenci (różne kierunki) pod względem stopnia zagrożenia systemu uczelni wyższej przez wykorzystanie luk w zabezpieczeniach do poczty elektronicznej i serwisu informacyjnego



Źródło: opracowanie własne na podstawie badań własnych

W związku z faktem, że wartość liczbowa w ocenie relacji jest dodatnia oznacza to, iż wraz ze wzrostem wartości jednej zmiennej rosną wartości także drugiej. Tabela 3.24. przedstawia odpowiedzi respondentów grupy kadra administracyjna i grupy studenci (różne kierunki) na temat zagrożeń systemu informacyjnego w uczelni wyższej przez wykorzystanie luk w zabezpieczeniach do poczty elektronicznej i serwisu informacyjnego.

Tabela 3.24. Odpowiedzi respondentów grupy kadra administracyjna i grupy studenci (różne kierunki) na temat zagrożeń systemu informacyjnego w uczelni wyższej przez wykorzystanie luk w zabezpieczeniach do poczty elektronicznej i serwisu informacyjnego

Odpowiedzi badanych osób wykorzystywanie luk w zabezpieczeniach dostępu do poczty elektronicznej i serwisu informacyjnego						
Osoby poddane badaniu	**Respondenci kadra administracyjna**		**Respondenci studenci (różne kierunki)**		**OGÓŁEM**	
Ocena	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***
bardzo niska	259	51,8%	162	32,4%	421	42,1%
niska	169	33,8%	255	51%	424	42,4%
przeciętna	46	9,2%	45	9%	91	9,1%
wysoka	23	4,6%	29	5,8%	52	5,2%
bardzo wysoka	3	3%	9	1,8%	12	1,2%
	500	**100%**	**500**	**100%**	**1000**	**100%**

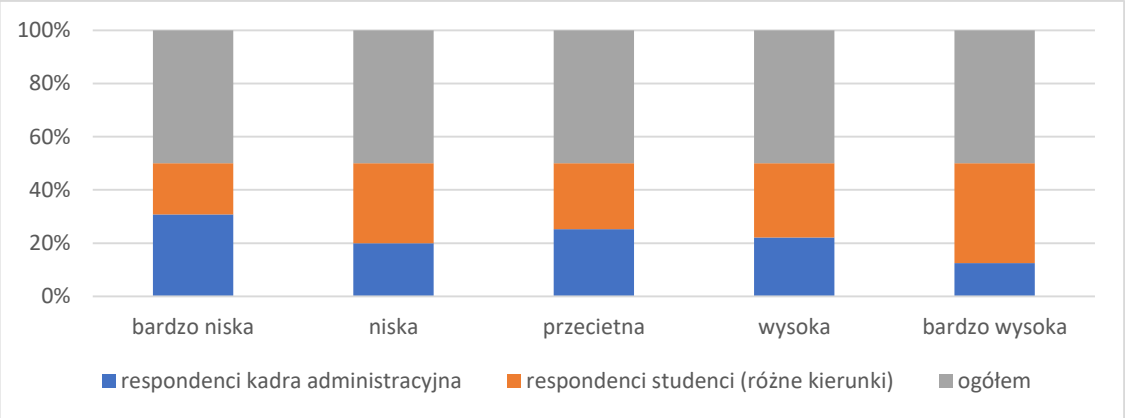
Źródło: opracowanie własne na podstawie badań własnych

W badaniu wzięło udział 500 osób zatrudnionych na stanowisku, kadry administracyjnej oraz 500 osób studiujących w uczelni wyższej. Z przeprowadzonej analizy wynika, że kadra administracyjna jak i studenci (różne kierunki) ocenili stopień zagrożenia systemu uczelni wyższej przez wykorzystanie luk w zabezpieczeniach do poczty elektronicznej i serwisu informacyjnego, jako bardzo niski i niski. Wskazuje na to 259 respondentów, co w udziale procentowym wynosi 51,8% dla kadry administracyjnej i 255 respondentów, co w udziale procentowym dla studentów (różne roczniki) wynosi 51%.

Analizując udzielone odpowiedzi w opinii 3 respondentów, co w udziale procentowym wynosi 3% dla kadry administracyjnej i 9 respondentów, co w udziale procentowym daje 1,8% dla studentów studiujących w uczelni wyższej świadczy, że pojawienie się wykorzystanie luk w zabezpieczeniach do poczty elektronicznej i serwisu informacyjnego stanowi bardzo duże zagrożenie dla systemu informacyjnego uczelni wyższej.

Wykres 3.47. przedstawia odpowiedzi respondentów grupy kadry administracyjnej i grupy studenci (różne kierunki) na temat stopnia zagrożenia systemu uczelni wyższej przez wykorzystanie luk w zabezpieczeniach do poczty elektronicznej i serwisu informacyjnego.

Wykres 3.47. Odpowiedzi respondentów grupy kadra administracyjna i grupy studenci (różne kierunki) na temat stopnia zagrożenia systemu uczelni wyższej przez wykorzystanie luk w zabezpieczeniach do poczty elektronicznej i serwisu informacyjnego



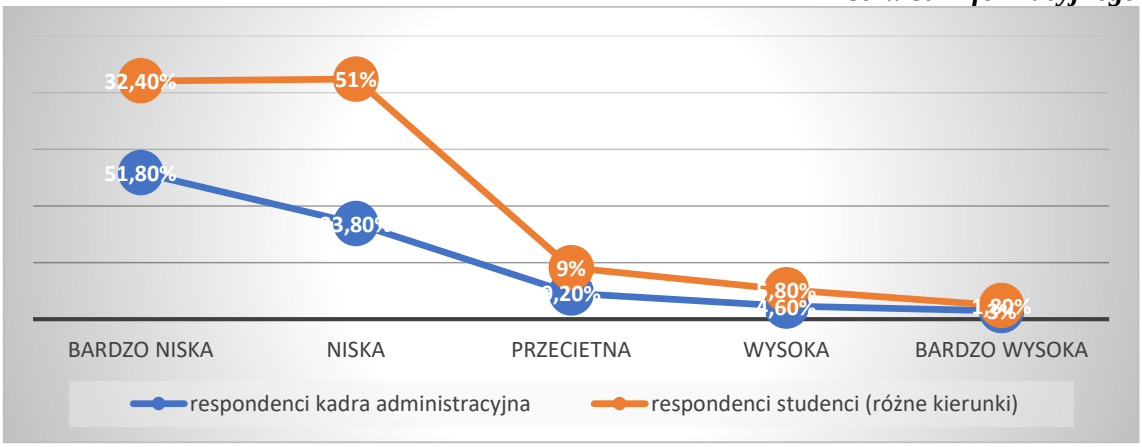
Źródło: opracowanie własne na podstawie badań własnych

O stopniu zależności świadczy współczynnik korelacji liniowej Pearsona na poziomie 0,82 i współczynnik determinacji liniowej, który wskazuje procent wyjaśnionej liniowo zmienności równy 67,24%. Wykres 3.48. pokazuje zależność między respondentami grupy kadra administracyjna grupy studenci (różne kierunki) pod względem stopnia zagrożenia systemu uczelni wyższej przez wykorzystanie luk w zabezpieczeniach do poczty elektronicznej i serwisu informacyjnego.

$$r_{xy} = \frac{\frac{1}{n}\sum_{i=1}^{n}(x_i-\bar{x})(y_i-\bar{y})}{S_x S_y}=0{,}82$$

$$\text{WD}=r_{xy}^{2} * 100\% = 67{,}24\%$$

Wykres 3.48. Zależność między respondentami grupy kadra administracyjna i grupy studenci (różne kierunki) pod względem stopnia zagrożenia systemu uczelni wyższej przez wykorzystanie luk w zabezpieczeniach do poczty elektronicznej i serwisu informacyjnego



Źródło: opracowanie własne na podstawie badań własnych

W związku z faktem, że wartość liczbowa w ocenie relacji jest dodatnia oznacza to, iż wraz ze wzrostem wartości jednej zmiennej rosną wartości także drugiej.

13. Jak Państwo oceniają zagrożenia systemu informacyjnego w uczelni wyższej?

i) Programy wykorzystujące błędy w systemach operacyjnych i oprogramowaniu użytkowym

Rozkład odpowiedzi respondentów grupy nauczycieli akademickich i kadry administracyjnej dotyczący oceny przez użytkowników stopnia zagrożenia systemu uczelni wyższej przez programy wykorzystujące błędy w systemach operacyjnych i w oprogramowaniu użytkowym zaprezentowano w tabeli 2.25.

Tabela 3.25. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy kadra administracyjna na temat zagrożeń systemu informacyjnego w uczelni wyższej przez programy wykorzystujące błędy w systemach operacyjnych i w oprogramowaniu użytkowym

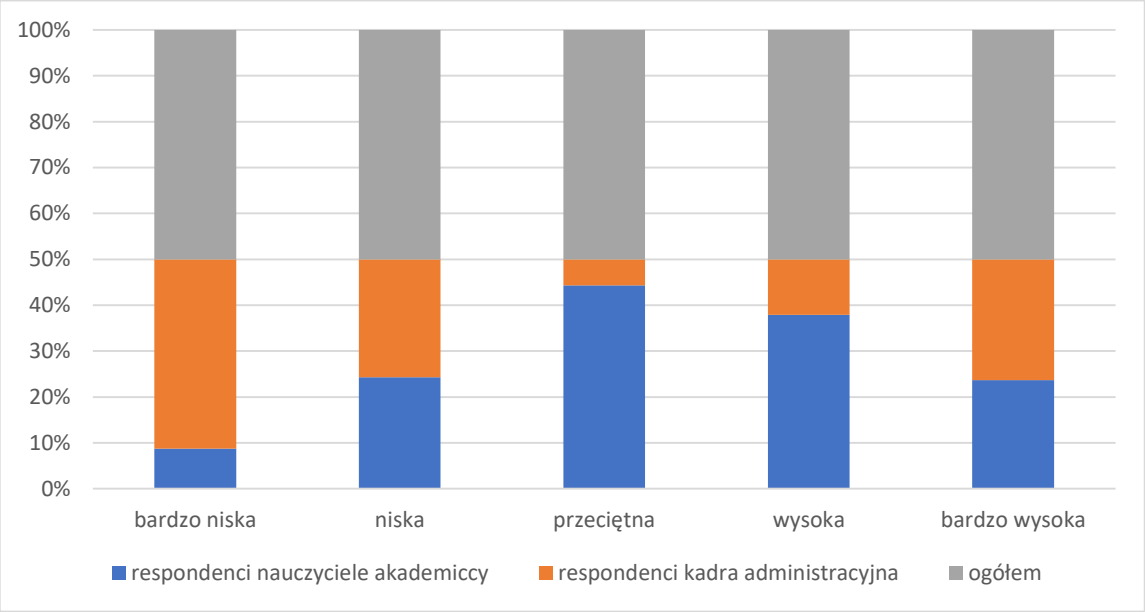
Odpowiedzi badanych osób programy wykorzystujące błędy w systemach operacyjnych i w oprogramowaniu użytkowym						
Osoby poddane badaniu	**Respondenci nauczyciele akademiccy**		**Respondenci kadra administracyjna**		**OGÓŁEM**	
Ocena	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***
bardzo niska	42	8,4%	198	39,6%	240	24%
niska	248	49,6%	262	52,4%	510	51%
przeciętna	179	35,8%	23	4,6%	202	20,2%
wysoka	22	4,4%	7	1,4%	29	2,9%
bardzo wysoka	9	1,8%	10	2%	19	1,9%
	500	**100%**	**500**	**100%**	**1000**	**100%**

Źródło: opracowanie własne na podstawie badań własnych

W badaniu wzięło udział 500 osób zatrudnionych na stanowisku, nauczycieli akademickich oraz 500 osób zatrudnionych na stanowisku kadra administracyjna. Z przeprowadzonej analizy wynika, że nauczyciele akademiccy jak i kadra administracyjna ocenili stopień zagrożenia systemu uczelni wyższej przez programy wykorzystujące błędy w systemach operacyjnych i w oprogramowaniu użytkowym, jako niski. Wskazuje na to 248 respondentów, co w udziale procentowym wynosi 49,6% dla nauczycieli akademickich i 262 respondentów, co w udziale procentowym dla kadry administracyjnej wynosi 39,6%.

Analizując udzielone odpowiedzi w opinii 9 respondentów, co w udziale procentowym wynosi 1,8% dla nauczycieli akademickich i 10 respondentów, co w udziale procentowym daje 2% dla kadry administracyjnej świadczy, że pojawienie się błędów w systemach operacyjnych i w oprogramowanych użytkowych stanowi bardzo duże zagrożenie dla systemu informacyjnego uczelni wyższej. Wykres 3.49. przedstawia odpowiedzi respondentów grupy nauczyciele akademiccy i grupy kadra administracyjna na temat stopnia zagrożenia systemu uczelni wyższej przez programy wykorzystujące błędy w systemach operacyjnych i w oprogramowaniu użytkowym.

Wykres 3.49. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy kadra administracyjna na temat stopnia zagrożenia systemu uczelni wyższej przez wykorzystujące błędy w systemach operacyjnych i w oprogramowaniu użytkowym



Źródło: opracowanie własne na podstawie badań własnych

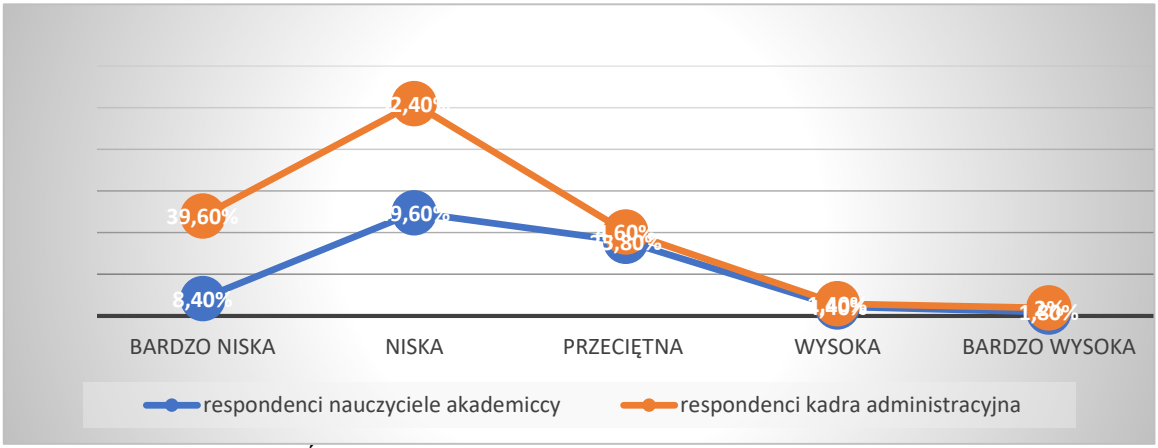
O stopniu zależności świadczy współczynnik korelacji liniowej Pearsona na poziomie 0,53 i współczynnik determinacji liniowej, który wskazuje procent wyjaśnionej liniowo zmienności równy 28,09%.

Wykres 3.50. pokazuje zależność między respondentami grupy nauczyciele akademiccy i grupy kadra administracyjna pod względem stopnia zagrożenia systemu uczelni wyższej przez programy wykorzystujące błędy w systemach operacyjnych i w oprogramowaniu użytkowym.

$$r_{xy} = \frac{\frac{1}{n}\sum_{i=1}^{n}(x_i-\bar{x})(y_i-\bar{y})}{S_x S_y}=0{,}53$$

$$\mathrm{WD}=r_{xy}^{2} * 100\% = 28{,}09\%$$

Wykres 3.50. Zależność między respondentami grupy nauczyciele akademiccy i grupy kadra administracyjna pod względem stopnia zagrożenia systemu uczelni wyższej przez programy wykorzystujące błędy w systemach operacyjnych i w oprogramowaniu użytkowym



Źródło: opracowanie własne na podstawie badań własnych

W związku z faktem, że wartość liczbowa w ocenie relacji jest dodatnia oznacza to, iż wraz ze wzrostem wartości jednej zmiennej rosną wartości także drugiej. Tabela 3.26. przedstawia odpowiedzi respondentów grupy nauczyciele akademiccy i grupy studenci (różne kierunki) na temat zagrożeń systemu informacyjnego w uczelni wyższej przez programy wykorzystujące błędy w systemach operacyjnych i w oprogramowaniu użytkowym.

Tabela 3.26. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy studenci (różne kierunki) na temat zagrożeń systemu informacyjnego w uczelni wyższej przez programy wykorzystujące błędy w systemach operacyjnych i w oprogramowaniu użytkowym

Odpowiedzi badanych osób programy wykorzystujące błędy w systemach operacyjnych i w oprogramowaniu użytkowym						
Osoby poddane badaniu	**Respondenci nauczyciele akademiccy**		**Respondenci studenci (różne kierunki)**		**OGÓŁEM**	
Ocena	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***
bardzo niska	42	8,4%	62	12,4%	104	10,4%
niska	248	49,6%	238	47,6%	486	48,6%
przeciętna	179	35,8%	168	33,6%	347	34,7%
wysoka	22	4,4%	26	5,2%	48	4,8%
bardzo wysoka	9	1,8%	6	1,2%	15	1,5%
	500	**100%**	**500**	**100%**	**1000**	**100%**

Źródło: opracowanie własne na podstawie badań własnych

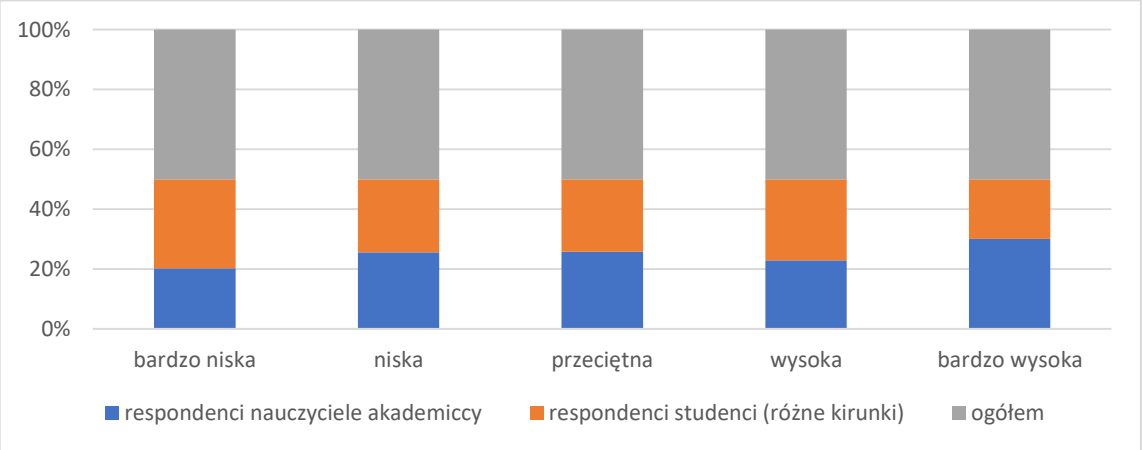
W badaniu wzięło udział 500 osób zatrudnionych na stanowisku, nauczycieli akademickich oraz 500 osób studiujących w uczelni wyższej. Z przeprowadzonej analizy

wynika, że nauczyciele akademiccy jak i studenci (różne kierunki) ocenili stopień zagrożenia systemu uczelni wyższej przez programy wykorzystujące błędy w systemach operacyjnych i w oprogramowaniu użytkowym, jako niski. Wskazuje na to 248 respondentów, co w udziale procentowym wynosi 49,6% dla nauczycieli akademickich i 238 respondentów, co w udziale procentowym dla studentów (różne roczniki) wynosi 47,6%.

Analizując udzielone odpowiedzi w opinii 9 respondentów, co w udziale procentowym wynosi 1,8% dla nauczycieli akademickich i 6 respondentów, co w udziale procentowym daje 1,2% dla studentów studiujących w uczelni wyższej świadczy, że pojawienie się programów wykorzystujących błędy w systemach operacyjnych i w oprogramowaniu użytkowym stanowi bardzo duże zagrożenie dla systemu informacyjnego uczelni wyższej.

Wykres 3.51. przedstawia odpowiedzi respondentów grupy nauczyciele akademiccy i grupy studenci na temat stopnia zagrożenia systemu uczelni wyższej przez programy wykorzystujące błędy w systemach operacyjnych i w oprogramowaniu użytkowym.

Wykres 3.51. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy studenci (różne kierunki) na temat stopnia zagrożenia systemu uczelni wyższej przez programy wykorzystujące błędy w systemach operacyjnych i w oprogramowaniu użytkowym



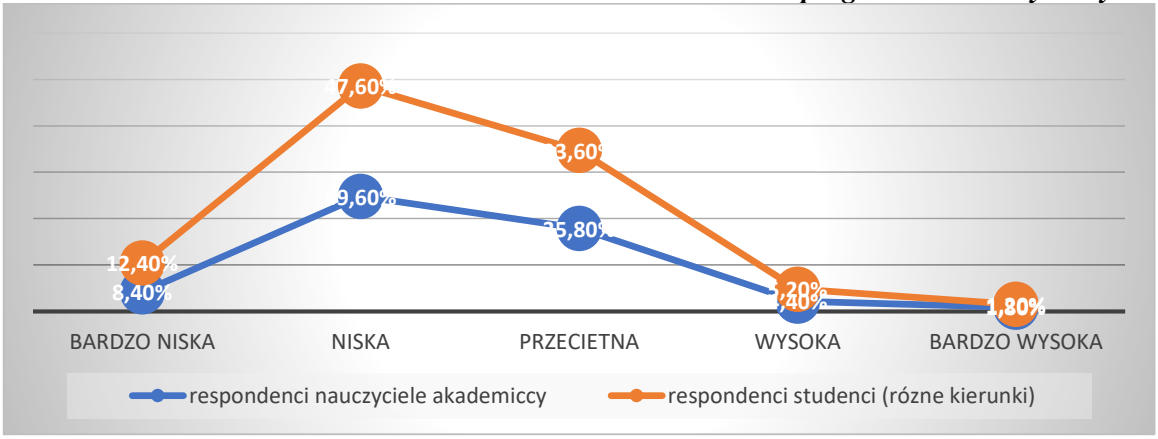
Źródło: opracowanie własne na podstawie badań własnych

O stopniu zależności świadczy współczynnik korelacji liniowej Pearsona na poziomie 0,99 i współczynnik determinacji liniowej, który wskazuje procent wyjaśnionej liniowo zmienności równy 98,01%. Wykres 3.52. pokazuje zależność między respondentami grupy nauczyciele akademiccy i grupy studenci (różne kierunki) pod względem stopnia zagrożenia systemu uczelni wyższej przez programy wykorzystujące błędy w systemach operacyjnych i w oprogramowaniu użytkowym.

$$r_{xy} = \frac{\frac{1}{n}\sum_{i=1}^{n}(x_i-\bar{x})(y_i-\bar{y})}{S_x S_y}=0{,}99$$

$$\text{WD}=r_{xy}^{2} * 100\% = 98{,}01\%$$

Wykres 3.52. Zależność między respondentami grupy nauczyciele akademiccy i grupy studenci (różne kierunki) pod względem stopnia zagrożenia systemu uczelni wyższej przez programy wykorzystujące błędy w systemach operacyjnych i w oprogramowaniu użytkowym



Źródło: opracowanie własne na podstawie badań własnych

W związku z faktem, że wartość liczbowa w ocenie relacji jest dodatnia oznacza to, iż wraz ze wzrostem wartości jednej zmiennej rosną wartości także drugiej. Tabela 3.27. przedstawia odpowiedzi respondentów grupy kadra administracyjna i grupy studenci (różne kierunki) na temat zagrożeń systemu informacyjnego w uczelni wyższej przez programy wykorzystujące błędy w systemach operacyjnych i w oprogramowaniu użytkowym.

Tabela 3.27. Odpowiedzi respondentów grupy kadra administracyjna i grupy studenci (różne kierunki) na temat zagrożeń systemu informacyjnego w uczelni wyższej przez programy wykorzystujące błędy w systemach operacyjnych i w oprogramowaniu użytkowym

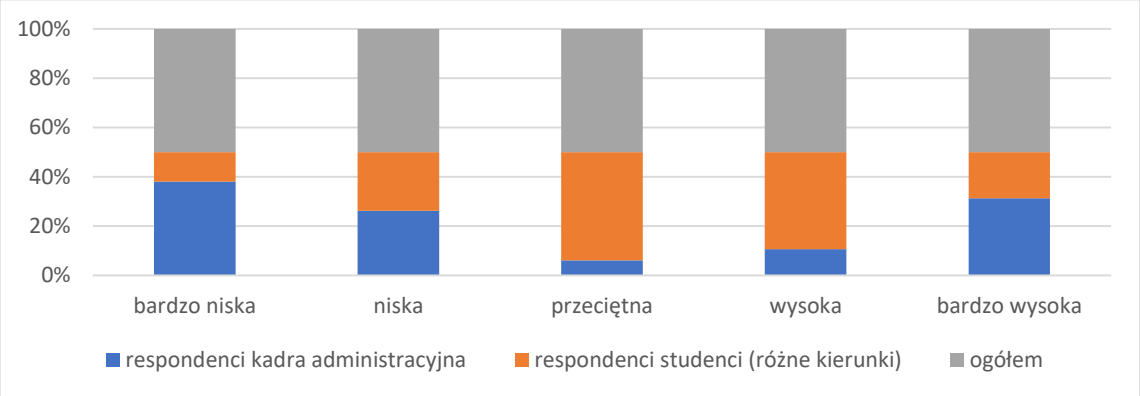
Odpowiedzi badanych osób programy wykorzystujące błędy w systemach operacyjnych i w oprogramowaniu użytkowym						
Osoby poddane badaniu	**Respondenci kadra administracyjna**		**Respondenci studenci (różne kierunki)**		**OGÓŁEM**	
Ocena	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***
bardzo niska	198	39,6%	62	12,4%	260	26%
niska	262	52,4%	238	47,6%	500	50%
przeciętna	23	4,6%	168	33,6%	191	19,1%
wysoka	7	1,4%	26	5,2%	33	3,3%
bardzo wysoka	10	2%	6	1,2%	16	1,6%
	500	**100%**	**500**	**100%**	**1000**	**100%**

Źródło: opracowanie własne na podstawie badań własnych

W badaniu wzięło udział 500 osób zatrudnionych na stanowisku, kadra administracyjna oraz 500 osób studiujących w uczelni wyższej. Z przeprowadzonej analizy wynika, że kadra administracyjna jak i studenci (różne kierunki) ocenili stopień zagrożenia systemu uczelni wyższej przez programy wykorzystujące błędy w systemach operacyjnych i w oprogramowaniu użytkowym, jako niski. Wskazuje na to 262 respondentów, co w udziale procentowym wynosi 52,4% dla kadry administracyjnej i 238 respondentów, co w udziale procentowym dla studentów (różne roczniki) wynosi 47,6%.

Analizując udzielone odpowiedzi w opinii 10 respondentów, co w udziale procentowym wynosi 2% dla kadry administracyjnej i 6 respondentów, co w udziale procentowym daje 1,2% dla studentów studiujących w uczelni wyższej świadczy, że pojawienie się programu wykorzystującego błędy w systemach operacyjnych i w oprogramowaniu użytkowym stanowi bardzo duże zagrożenie dla systemu informacyjnego uczelni wyższej. Wykres 3.53. przedstawia odpowiedzi respondentów grupy kadra administracyjna i grupy studenci (różne kierunki) na temat stopnia zagrożenia systemu uczelni wyższej przez programy wykorzystujące błędy w systemach operacyjnych i w oprogramowaniu użytkowym.

Wykres 3.53. Odpowiedzi respondentów grupy kadra administracyjna i grupy studenci (różne kierunki) na temat stopnia zagrożenia systemu uczelni wyższej przez programy wykorzystujące błędy w systemach operacyjnych i w oprogramowaniu użytkowym



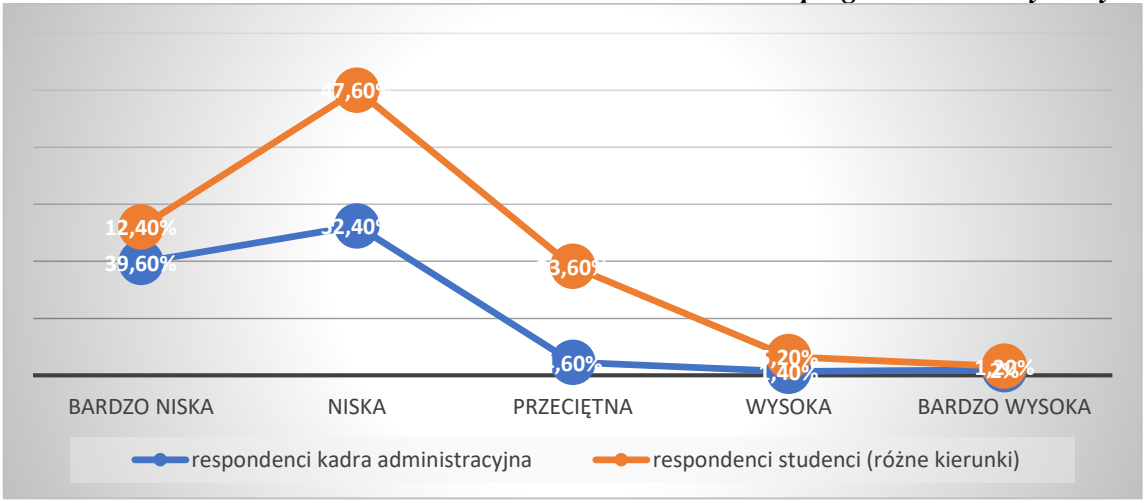
Źródło: opracowanie własne na podstawie badań własnych

O stopniu zależności świadczy współczynnik korelacji liniowej Pearsona na poziomie 0,60 i współczynnik determinacji liniowej, który wskazuje procent wyjaśnionej liniowo zmienności równy 36%. Wykres 3.54. pokazuje zależność między respondentami grupy kadra administracyjna i grupy studenci (różne kierunki) pod względem stopnia zagrożenia systemu uczelni wyższej przez programy wykorzystujące błędy w systemach operacyjnych i w oprogramowaniu użytkowym.

$$r_{xy} = \frac{\frac{1}{n}\sum_{i=1}^{n}(x_i-\bar{x})(y_i-\bar{y})}{S_x S_y}=0{,}60$$

$$\text{WD}=r\frac{2}{xy} * 100\% = 36\%$$

Wykres 3.54. Zależność między respondentami grupy kadra administracyjna i grupy studenci (różne kierunki) pod względem stopnia zagrożenia systemu uczelni wyższej przez programy wykorzystujące błędy w systemach operacyjnych i w oprogramowaniu użytkowym



Źródło: opracowanie własne na podstawie badań własnych

W związku z faktem, że wartość liczbowa w ocenie relacji jest dodatnia oznacza to, iż wraz ze wzrostem wartości jednej zmiennej rosną wartości także drugiej.

13. Jak Państwo oceniają zagrożenia systemu informacyjnego w uczelni wyższej?

j) Wirusy, robaki, konie trojańskie

Rozkład odpowiedzi respondentów grupy nauczycieli akademickich i kadry administracyjnej dotyczący oceny przez użytkowników stopnia zagrożenia systemu uczelni wyższej przez wirusy, robaki, konie trojańskie, zaprezentowane zostało w tabeli 3.28.

Tabela 3.28. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy kadra administracyjna na temat zagrożeń systemu informacyjnego w uczelni wyższej przez wirusy, robaki, konie trojańskie

Odpowiedzi badanych osób wirusy, robaki, konie trojańskie						
Osoby poddane badaniu	**Respondenci nauczyciele akademiccy**		**Respondenci kadra administracyjna**		**OGÓŁEM**	
Ocena	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***
bardzo niska	162	32,4%	59	11,8%	221	22,1%
niska	243	48,6%	265	53%	508	50,8%

przeciętna	39	7,8%	129	25,8%	168	16,8%
wysoka	27	5,4%	38	7,6%	65	6,5%
bardzo wysoka	29	5,8%	9	1,8%	38	3,8%
	500	**100%**	**500**	**100%**	**1000**	**100%**

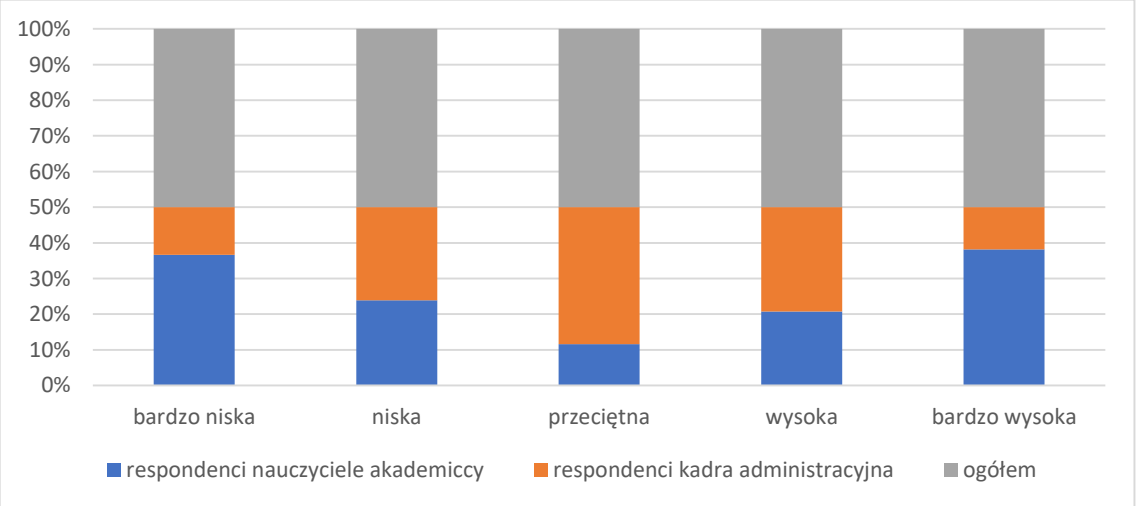
Źródło: opracowanie własne na podstawie badań własnych

W badaniu wzięło udział 500 osób zatrudnionych na stanowisku, nauczycieli akademickich oraz 500 osób zatrudnionych na stanowisku kadra administracyjna. Z przeprowadzonej analizy wynika, że nauczyciele akademiccy jak i kadra administracyjna ocenili stopień zagrożenia systemu uczelni wyższej przez wirusy, robaki, konie trojańskie jako niski. Wskazuje na to 243 respondentów, co w udziale procentowym wynosi 48,6% dla nauczycieli akademickich i 265 respondentów, co w udziale procentowym dla kadry administracyjnej wynosi 53%.

Analizując udzielone odpowiedzi w opinii 29 respondentów, co w udziale procentowym wynosi 5,8% dla nauczycieli akademickich i 9 respondentów, co w udziale procentowym daje 1,8% dla kadry administracyjnej świadczy, że pojawienie się wirusów, robaków, koni trojańskich stanowi bardzo duże zagrożenie dla systemu informacyjnego uczelni wyższej.

Wykres 3.55. przedstawia odpowiedzi respondentów grupy nauczyciele akademiccy i grupy kadra administracyjna na temat stopnia zagrożenia systemu uczelni wyższej przez wirusy, robaki, konie trojańskie.

Wykres 3.55. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy kadra administracyjna na temat stopnia zagrożenia systemu uczelni wyższej przez wirusy, robaki, konie trojańskie



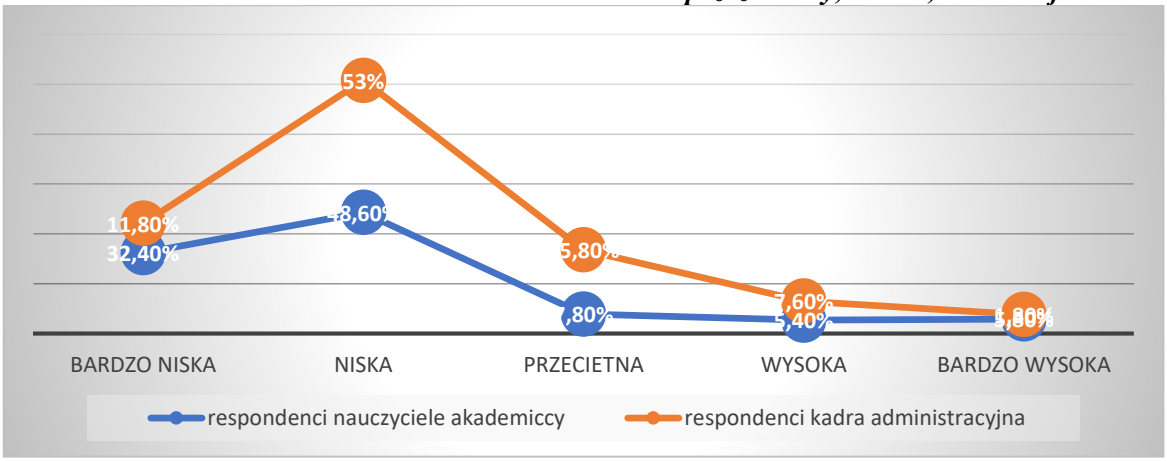
Źródło: opracowanie własne na podstawie badań własnych

O stopniu zależności świadczy współczynnik korelacji liniowej Pearsona na poziomie 0,75 i współczynnik determinacji liniowej, który wskazuje procent wyjaśnionej liniowo zmienności równy 56,25%. Wykres 3.56. pokazuje zależność między respondentami grupy nauczyciele akademiccy i grupy kadra administracyjna pod względem stopnia zagrożenia systemu uczelni wyższej przez wirusy, robaki, konie trojańskie.

$$r_{xy} = \frac{\frac{1}{n}\sum_{i=1}^{n}(x_i-\bar{x})(y_i-\bar{y})}{S_x S_y}=0{,}75$$

$$\text{WD}=r_{xy}^{2} * 100\% = 56{,}25\%$$

Wykres 3.56. Zależność między respondentami grupy nauczyciele akademiccy i grupy kadra administracyjna pod względem stopnia zagrożenia systemu uczelni wyższej przez wirusy, robaki, konie trojańskie



Źródło: opracowanie własne na podstawie badań własnych

W związku z faktem, że wartość liczbowa w ocenie relacji jest dodatnia oznacza to, iż wraz ze wzrostem wartości jednej zmiennej rosną wartości także drugiej. Tabela 3.29. przedstawia odpowiedzi respondentów grupy nauczyciele akademiccy i grupy studenci (różne kierunki) na temat zagrożeń systemu informacyjnego w uczelni wyższej przez wirusy, robaki, konie trojańskie.

Tabela 3.29. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy studenci (różne kierunki)na temat stopnia zagrożenia systemu uczelni wyższej przez wirusy, robaki, konie trojańskie

Odpowiedzi badanych osób wirusy, robaki, konie trojańskie						
Osoby poddane badaniu	**Respondenci nauczyciele akademiccy**		**Respondenci studenci (różne kierunki)**		**OGÓŁEM**	
Ocena	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***
bardzo niska	162	32,4%	45	9%	207	20,7%
niska	243	48,6%	289	57,8%	532	53,2%
przeciętna	39	7,8%	123	24,6%	162	16,2%
wysoka	27	5,4%	32	6,4%	59	5,9%

bardzo wysoka	29	5,8%	11	2,2%	40	4%
	500	**100%**	**500**	**100%**	**1000**	**100%**

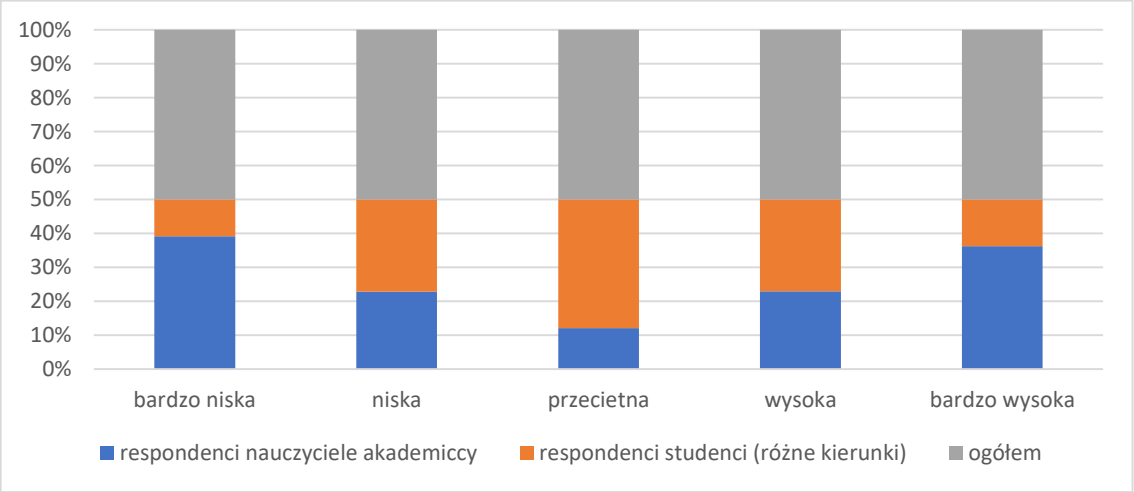
Źródło: opracowanie własne na podstawie badań własnych

W badaniu wzięło udział 500 osób zatrudnionych na stanowisku, nauczycieli akademickich oraz 500 osób studiujących w uczelni wyższej. Z przeprowadzonej analizy wynika, że nauczyciele akademiccy jak i studenci (różne kierunki) ocenili stopień zagrożenia systemu uczelni wyższej przez wirusy, robaki, konie trojańskie, jako niski. Wskazuje na to 243 respondentów, co w udziale procentowym wynosi 48,6% dla nauczycieli akademickich i 289 respondentów, co w udziale procentowym dla studentów (różne roczniki) wynosi 57,8%.

Analizując udzielone odpowiedzi w opinii 29 respondentów, co w udziale procentowym wynosi 5,8% dla nauczycieli akademickich i 11 respondentów, co w udziale procentowym daje 2,2% dla studentów studiujących w uczelni wyższej świadczy, że pojawienie się wirusów, robaków, koni trojańskich stanowi bardzo duże zagrożenie dla systemu informacyjnego uczelni wyższej.

Wykres 3.57. przedstawia odpowiedzi respondentów grupy nauczyciele akademiccy i grupy studenci na temat stopnia zagrożenia systemu uczelni wyższej przez wirusy, robaki, konie trojańskie.

Wykres 3.57. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy studenci (różne kierunki) na temat stopnia zagrożenia systemu uczelni wyższej przez wirusy, robaki, konie trojańskie



Źródło: opracowanie własne na podstawie badań własnych

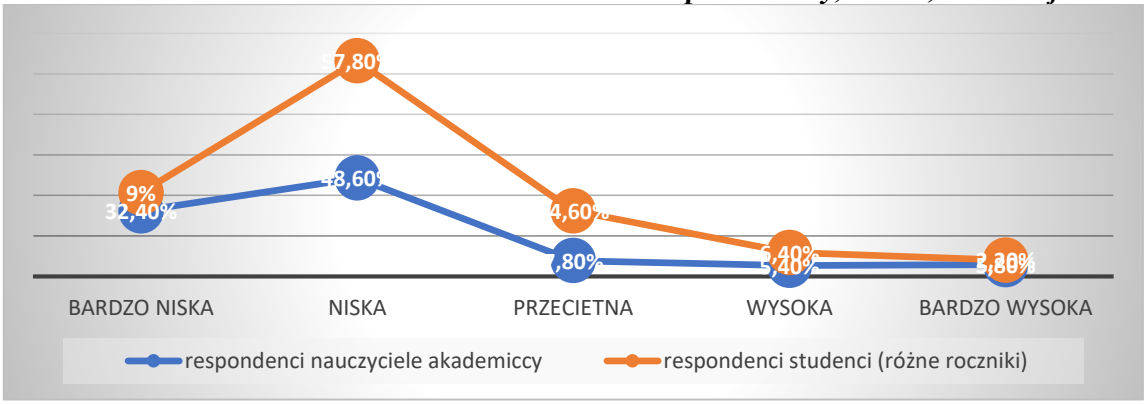
O stopniu zależności świadczy współczynnik korelacji liniowej Pearsona na poziomie 0,75 i współczynnik determinacji liniowej, który wskazuje procent wyjaśnionej

liniowo zmienności równy 56,25%. Wykres 3.58. pokazuje zależność między respondentami grupy nauczyciele akademiccy i grupy studenci (różne kierunki) pod względem stopnia zagrożenia systemu uczelni wyższej przez wirusy, robaki, konie trojańskie.

$$r_{xy} = \frac{\frac{1}{n}\sum_{i=1}^{n}(x_i-\bar{x})(y_i-\bar{y})}{S_x S_y}=0{,}75$$

$$\text{WD}=r_{xy}^{2} * 100\% = 56{,}25\%$$

Wykres 3.58. Zależności respondentów grupy nauczyciele akademiccy i grupy studenci (różne kierunki) na temat stopnia zagrożenia systemu uczelni wyższej przez wirusy, robaki, konie trojańskie



Źródło: opracowanie własne na podstawie badań własnych

W związku z faktem, że wartość liczbowa w ocenie relacji jest dodatnia oznacza to, iż wraz ze wzrostem wartości jednej zmiennej rosną wartości także drugiej. Tabela 3.30. przedstawia odpowiedzi respondentów grupy kadra administracyjna i grupy studenci (różne kierunki) na temat zagrożeń systemu informacyjnego w uczelni wyższej przez wirusy, robaki, konie trojańskie.

Tabela 3.30. Odpowiedzi respondentów grupy kadra administracyjna i grupy studenci (różne kierunki) na temat zagrożeń systemu informacyjnego w uczelni wyższej przez wirusy, robaki, konie trojańskie

Odpowiedzi badanych osób wirusy, robaki, konie trojańskie						
Osoby poddane badaniu	**Respondenci kadra administracyjna**		**Respondenci studenci (różne kierunki)**		**OGÓŁEM**	
Ocena	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***
bardzo niska	59	11,8%	45	9%	104	10,4%
niska	265	53%	289	57,8%	554	55,4%
przeciętna	129	25,8%	123	24,6%	252	25,2%
wysoka	38	7,6%	32	6,4%	70	7%
bardzo wysoka	9	1,8%	11	2,2%	20	2%
	500	**100%**	**500**	**100%**	**1000**	**100%**

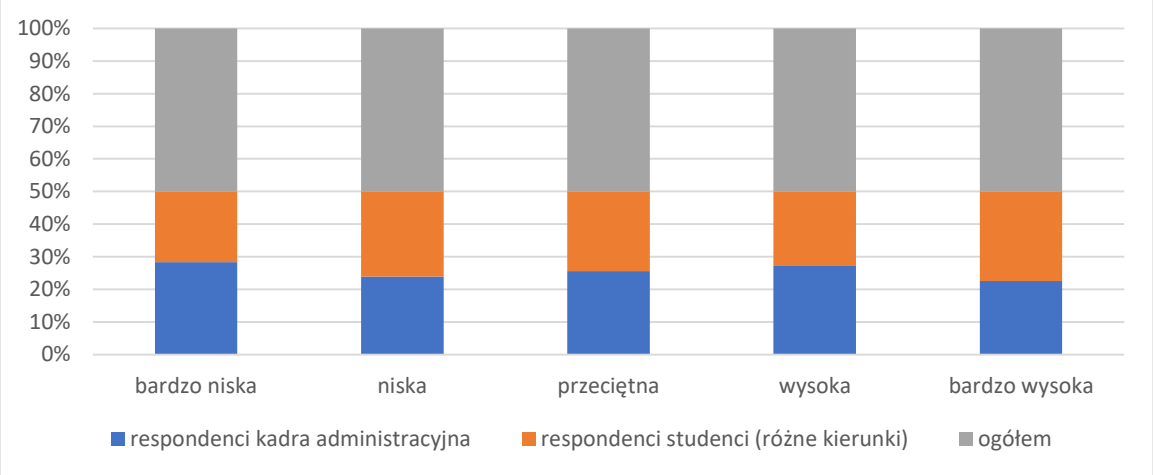
Źródło: opracowanie własne na podstawie badań własnych

W badaniu wzięło udział 500 osób zatrudnionych na stanowisku, kadra administracyjna oraz 500 osób studiujących w uczelni wyższej. Z przeprowadzonej analizy wynika, że kadra administracyjna jak i studenci (różne kierunki) ocenili stopień zagrożenia systemu uczelni wyższej przez wirusy, robaki, konie trojańskie, jako niski. Wskazuje na to 265 respondentów, co w udziale procentowym wynosi 53% dla kadry administracyjnej i 289 respondentów, co w udziale procentowym dla studentów (różne roczniki) wynosi 57,8%.

Analizując udzielone odpowiedzi w opinii 9 respondentów, co w udziale procentowym wynosi 1,8% dla kadry administracyjnej i 11 respondentów, co w udziale procentowym daje 2,2% dla studentów studiujących w uczelni wyższej świadczy, że pojawienie się wirusów, robaków, koni trojańskich stanowi bardzo duże zagrożenie dla systemu informacyjnego uczelni wyższej.

Wykres 3.59. przedstawia odpowiedzi respondentów grupy kadry administracyjnej i grupy studentów (różnych kierunków) na temat stopnia zagrożenia systemu uczelni wyższej przez wirusy, robaki, konie trojańskie.

Wykres 3.59. Odpowiedzi respondentów grupy kadra administracyjna i grupy studenci (różne kierunki) na temat stopnia zagrożenia systemu uczelni wyższej przez wirusy, robaki, konie trojańskie



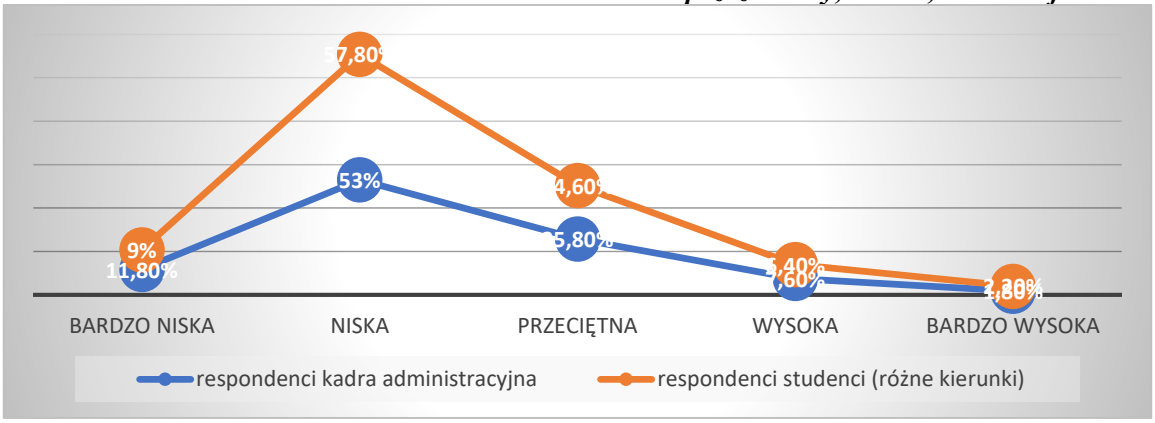
Źródło: opracowanie własne na podstawie badań własnych

O stopniu zależności świadczy współczynnik korelacji liniowej Pearsona na poziomie 0,99 i współczynnik determinacji liniowej, który wskazuje procent wyjaśnionej liniowo zmienności równy 98,01%. Wykres 3.60. pokazuje zależność między respondentami grupy kadra administracyjna i grupy studenci (różne kierunki) pod względem stopnia zagrożenia systemu uczelni wyższej przez wirusy, robaki, konie trojańskie.

$$r_{xy} = \frac{\frac{1}{n}\sum_{i=1}^{n}(x_i-\bar{x})(y_i-\bar{y})}{S_x S_y}=0{,}99$$

$$\text{WD}=r_{xy}^{2} * 100\% = 98{,}01\%$$

Wykres 3.60. Zależność między respondentami grupy kadra administracyjna i grupy studenci (różne kierunki) pod względem stopnia zagrożenia systemu uczelni wyższej przez wirusy, robaki, konie trojańskie



Źródło: opracowanie własne na podstawie badań własnych

W związku z faktem, że wartość liczbowa w ocenie relacji jest dodatnia oznacza to, iż wraz ze wzrostem wartości jednej zmiennej rosną wartości także drugiej.

13. Jak Państwo oceniają zagrożenia systemu informacyjnego w uczelni wyższej?

k) Obecność podejrzanego oprogramowania

Rozkład odpowiedzi respondentów grupy nauczyciele akademiccy i grupy kadra administracyjna dotyczący oceny przez użytkowników stopnia zagrożenia systemu uczelni wyższej przez obecność podejrzanego oprogramowania prezentuje tabela 3.31.

Tabela 3.31. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy kadra administracyjna na temat zagrożeń systemu informacyjnego w uczelni wyższej przez obecność podejrzanego oprogramowania

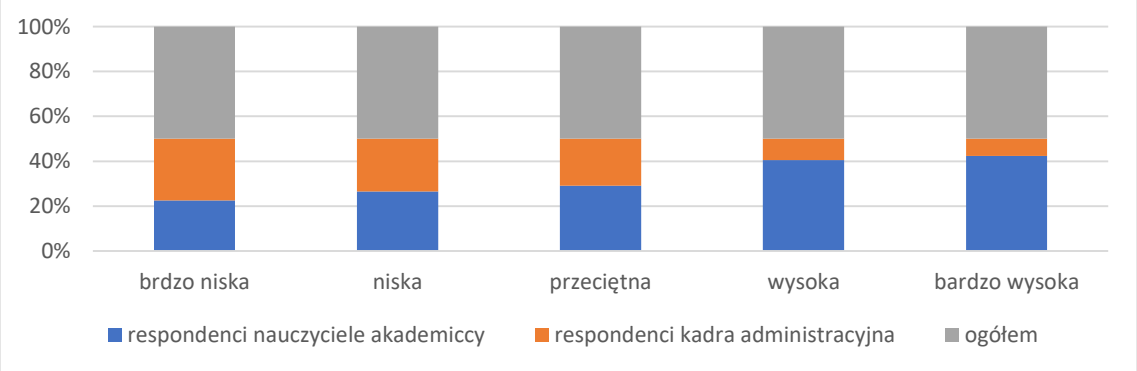
Odpowiedzi badanych osób obecność podejrzanego oprogramowania						
Osoby poddane badaniu	**Respondenci nauczyciele akademiccy**		**Respondenci kadra administracyjna**		**OGÓŁEM**	
Ocena	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***
bardzo niska	244	48,8%	298	59,6%	542	54,2%
niska	189	37,8%	168	33,6%	357	35,7%
przeciętna	39	7,8%	28	5,6%	67	6,7%
wysoka	17	3,4%	4	0,8%	21	2,1%
bardzo wysoka	11	2,2%	2	0,4%	13	1,3%
	500	**100%**	**500**	**100%**	**1000**	**100%**

Źródło: opracowanie własne na podstawie badań własnych

W badaniu wzięło udział 500 osób zatrudnionych na stanowisku, nauczycieli akademickich oraz 500 osób zatrudnionych na stanowisku kadra administracyjna. Z przeprowadzonej analizy wynika, że nauczyciele akademiccy jak i kadra administracyjna ocenili stopień zagrożenia systemu uczelni wyższej przez obecność podejrzanego oprogramowania, jako bardzo niski. Wskazuje na to 244 respondentów, co w udziale procentowym wynosi 48,8% dla nauczycieli akademickich i 298 respondentów, co w udziale procentowym dla kadry administracyjnej wynosi 59,6%.

Analizując udzielone odpowiedzi w opinii 11 respondentów, co w udziale procentowym wynosi 2,2% dla nauczycieli akademickich i 2 respondentów, co w udziale procentowym daje 0,4% dla kadry administracyjnej świadczy, że pojawienie się obecności podejrzanego oprogramowania stanowi bardzo duże zagrożenie dla systemu informacyjnego uczelni wyższej. Wykres 3.61. przedstawia odpowiedzi respondentów grupy nauczyciele akademiccy i grupy kadra administracyjna na temat stopnia zagrożenia systemu uczelni wyższej przez obecność podejrzanego oprogramowania.

Wykres 3.61. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy kadra administracyjna na temat stopnia zagrożenia systemu uczelni wyższej przez obecność podejrzanego oprogramowania



Źródło: opracowanie własne na podstawie badań własnych

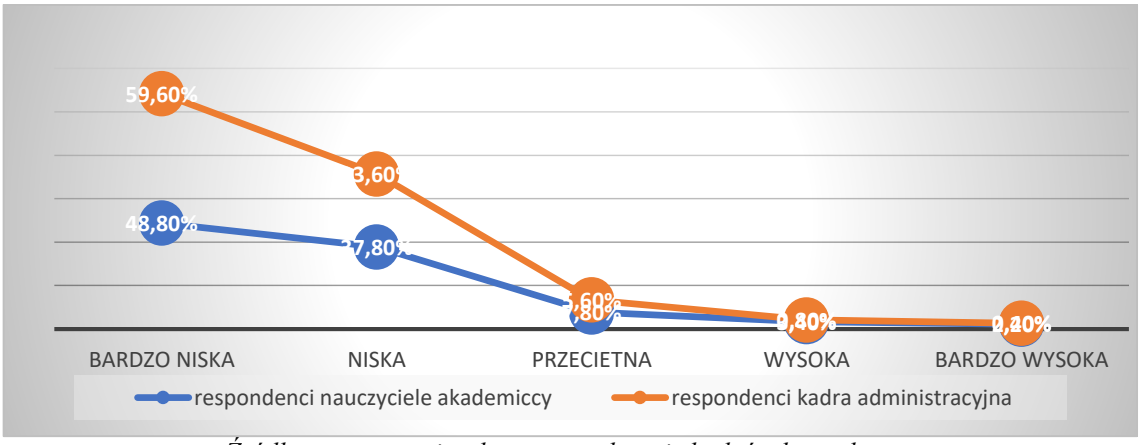
O stopniu zależności świadczy współczynnik korelacji liniowej Pearsona na poziomie 0,98 i współczynnik determinacji liniowej, który wskazuje procent wyjaśnionej liniowo zmienności równy 96,04%.

Wykres 3.62. pokazuje zależność między respondentami grupy nauczyciele akademiccy i grupy kadra administracyjna pod względem stopnia zagrożenia systemu uczelni wyższej przez obecność podejrzanego oprogramowania.

$$r_{xy} = \frac{\frac{1}{n}\sum_{i=1}^{n}(x_i-\bar{x})(y_i-\bar{y})}{S_x S_y}=0{,}98$$

$$\mathrm{WD}=r_{xy}^{2} * 100\% = 96{,}04\%$$

Wykres 3.62. Zależność między respondentami grupy nauczyciele akademiccy i grupy kadra administracyjna pod względem stopnia zagrożenia systemu uczelni wyższej przez obecność podejrzanego oprogramowania



Źródło: opracowanie własne na podstawie badań własnych

W związku z faktem, że wartość liczbowa w ocenie relacji jest dodatnia oznacza to, iż wraz ze wzrostem wartości jednej zmiennej rosną wartości także drugiej. Tabela 3.32. przedstawia odpowiedzi respondentów grupy nauczyciele akademiccy i grupy studenci na temat zagrożeń systemu informacyjnego w uczelni wyższej przez obecność podejrzanego oprogramowania.

Tabela 3.32. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy studenci (różne kierunki) na temat zagrożeń systemu informacyjnego w uczelni wyższej przez obecność podejrzanego oprogramowania

Odpowiedzi badanych osób obecność podejrzanego oprogramowania						
Osoby poddane badaniu	**Respondenci nauczyciele akademiccy**		**Respondenci studenci (różne kierunki)**		**OGÓŁEM**	
Ocena	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***
bardzo niska	244	48,8%	169	33,8%	413	41,3%
niska	189	37,8%	312	62,4%	501	50,1%
przeciętna	39	7,8%	17	3,4%	56	5,6%
wysoka	17	3,4%	2	0,4%	19	1,9%
bardzo wysoka	11	2,2%	0	0,0%	11	11%
	500	**100%**	**500**	**100%**	**1000**	**100%**

Źródło: opracowanie własne na podstawie badań własnych

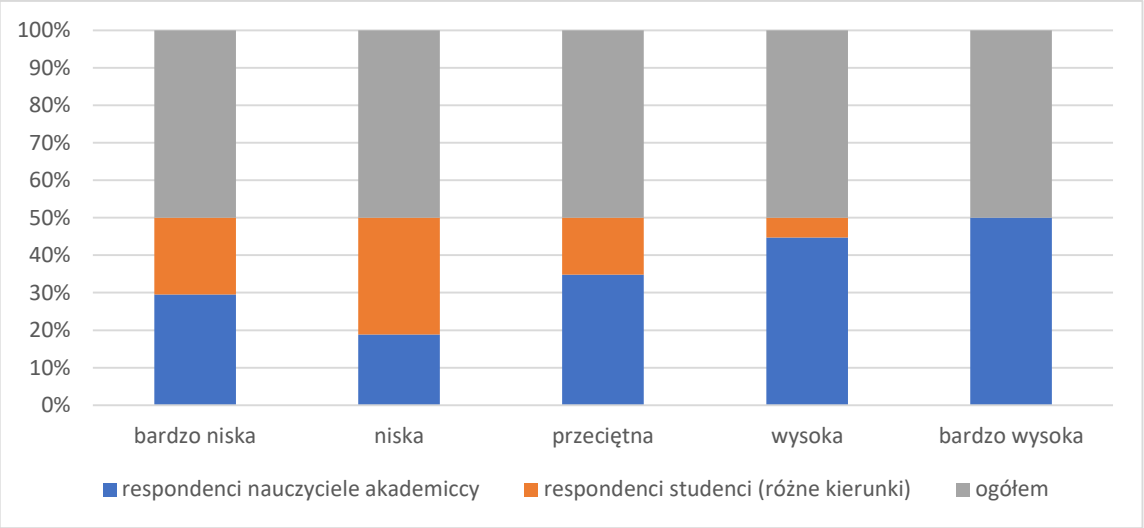
W badaniu wzięło udział 500 osób zatrudnionych na stanowisku, nauczycieli akademickich oraz 500 osób studiujących w uczelni wyższej. Z przeprowadzonej analizy wynika, że nauczyciele akademiccy jak i studenci (różne kierunki) ocenili stopień zagro-

żenia systemu uczelni wyższej przez obecność podejrzanego oprogramowania, jako bardzo niski i niski. Wskazuje na to 244 respondentów, co w udziale procentowym wynosi 48,8% dla nauczycieli akademickich i 312 respondentów, co w udziale procentowym dla studentów (różne roczniki) wynosi 33,8%.

Analizując udzielone odpowiedzi w opinii 11 respondentów, co w udziale procentowym wynosi 2,2% dla nauczycieli akademickich i 0 respondentów, co w udziale procentowym daje 0% dla studentów studiujących w uczelni wyższej świadczy, że pojawienie się podejrzanego oprogramowania stanowi bardzo duże zagrożenie dla systemu informacyjnego uczelni wyższej.

Wykres 3.63. przedstawia odpowiedzi respondentów grupy nauczyciele akademiccy i grupy studentów (różne kierunki) na temat stopnia zagrożenia systemu uczelni wyższej przez obecność podejrzanego oprogramowania.

Wykres 3.63. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy studenci (różne kierunki) na temat stopnia zagrożenia systemu uczelni wyższej przez obecność podejrzanego oprogramowania



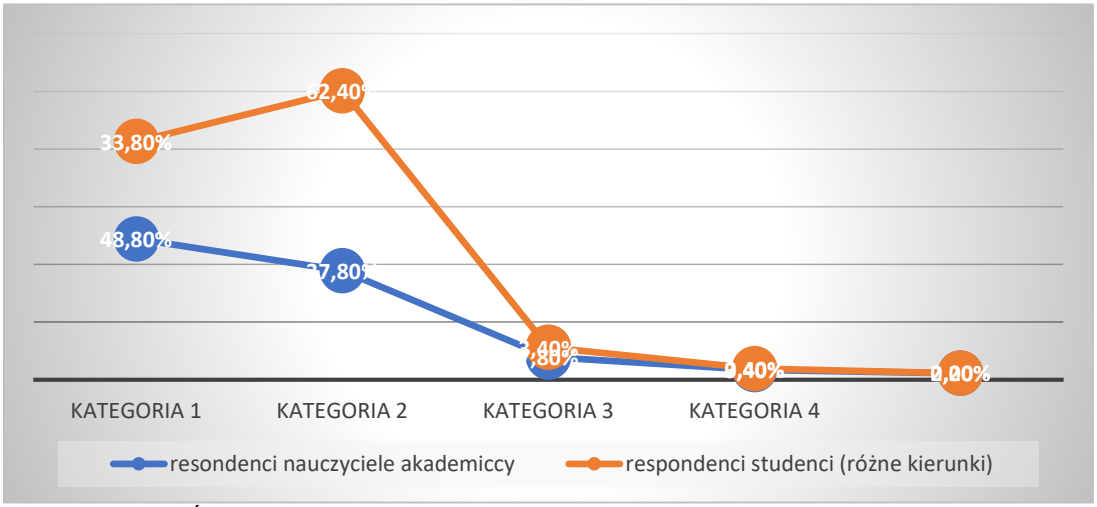
Źródło: opracowanie własne na podstawie badań własnych

O stopniu zależności świadczy współczynnik korelacji liniowej Pearsona na poziomie 0,85 i współczynnik determinacji liniowej, który wskazuje procent wyjaśnionej liniowo zmienności równy 72,25%. Wykres 3.64. pokazuje zależność między respondentami grupy nauczyciele akademiccy i grupy studenci (różne kierunki) pod względem stopnia zagrożenia systemu uczelni wyższej przez obecność podejrzanego oprogramowania.

$$r_{xy} = \frac{\frac{1}{n}\sum_{i=1}^{n}(x_i-\bar{x})(y_i-\bar{y})}{S_x S_y}=0{,}85$$

$$\mathrm{WD}=r_{xy}^{2} * 100\% = 72{,}25\%$$

Wykres 3.64. Zależność między respondentami grupy nauczyciele akademiccy i grupy studenci (różne kierunki) pod względem stopnia zagrożenia systemu uczelni wyższej przez obecność podejrzanego oprogramowania



Źródło: opracowanie własne na podstawie badań własnych

W związku z faktem, że wartość liczbowa w ocenie relacji jest dodatnia oznacza to, iż wraz ze wzrostem wartości jednej zmiennej rosną wartości także drugiej. Tabela 3.33. przedstawia odpowiedzi respondentów grupy kadra administracyjna i grupy studenci (różne kierunki) na temat zagrożeń systemu informacyjnego w uczelni wyższej przez obecność podejrzanego oprogramowania.

Tabela 3.33. Odpowiedzi respondentów grupy kadra administracyjna i grupy studenci (różne kierunki) na temat zagrożeń systemu informacyjnego w uczelni wyższej przez obecność podejrzanego oprogramowania

Odpowiedzi badanych osób obecność podejrzanego oprogramowania						
Osoby poddane badaniu	**Respondenci kadra administracyjna**		**Respondenci studenci (różne kierunki)**		**OGÓŁEM**	
Ocena	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***
bardzo niska	298	59,6%	169	33,8%	467	46,7%
niska	168	33,6%	312	62,4%	480	48%
przeciętna	28	5,6%	17	3,4%	45	4,5%
wysoka	4	0,8%	2	0,4%	6	0,6%
bardzo wysoka	2	0,4%	0	0,0%	2	0,2%
	500	**100%**	**500**	**100%**	**1000**	**100%**

Źródło: opracowanie własne na podstawie badań własnych

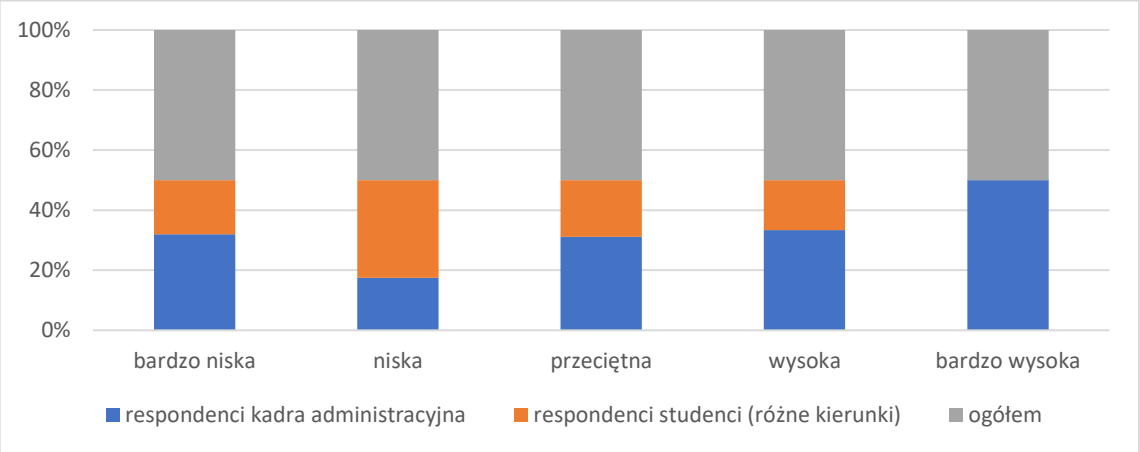
W badaniu wzięło udział 500 osób zatrudnionych na stanowisku, kadra administracyjna oraz 500 osób studiujących w uczelni wyższej. Z przeprowadzonej analizy wynika, że kadra administracyjna jak i studenci (różne kierunki) ocenili stopień zagrożenia

systemu uczelni wyższej przez obecność podejrzanego oprogramowania, jako bardzo niski i niski. Wskazuje na to 298 respondentów, co w udziale procentowym wynosi 59,6% dla kadry administracyjnej i 312 respondentów, co w udziale procentowym dla studentów (różne roczniki) wynosi 62,4%.

Analizując udzielone odpowiedzi w opinii 2 respondentów, co w udziale procentowym wynosi 0,4% dla kadry administracyjnej i 0 respondentów, co w udziale procentowym daje 0% dla studentów studiujących w uczelni wyższej świadczy, że pojawienie się obecności podejrzanego oprogramowania stanowi bardzo duże zagrożenie dla systemu informacyjnego uczelni wyższej.

Wykres 3.65. przedstawia odpowiedzi respondentów grupy kadry administracyjnej i grupy studentów (różnych kierunków) na temat stopnia zagrożenia systemu uczelni wyższej przez obecność podejrzanego oprogramowania.

Wykres 3.65. Odpowiedzi respondentów grupy kadra administracyjna i grupy studenci (różne kierunki) na temat stopnia zagrożenia systemu uczelni wyższej przez obecność podejrzanego oprogramowania



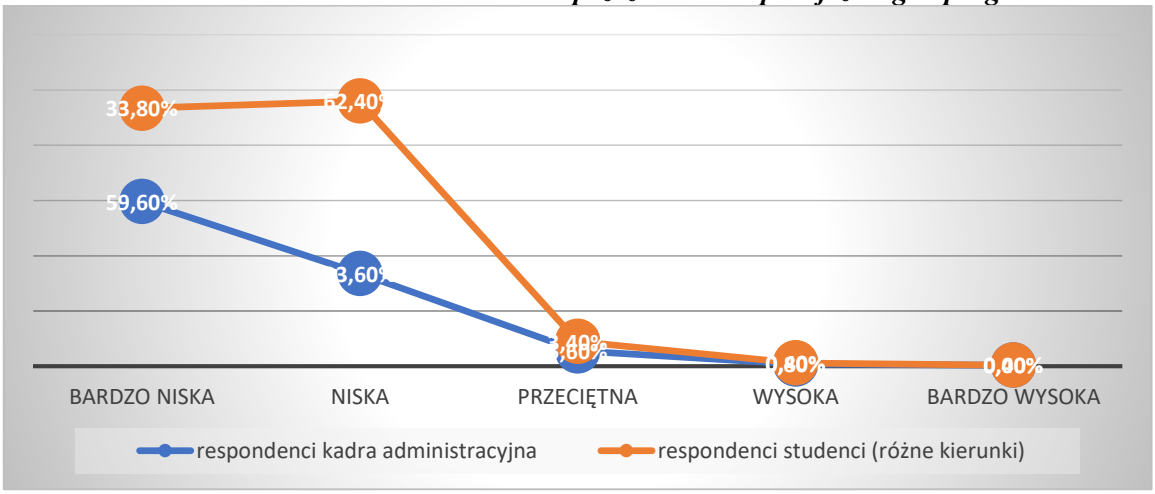
Źródło: opracowanie własne na podstawie badań własnych

O stopniu zależności świadczy współczynnik korelacji liniowej Pearsona na poziomie 0,74 i współczynnik determinacji liniowej, który wskazuje procent wyjaśnionej liniowo zmienności równy 54,76%. Wykres 3.66. pokazuje zależność między respondentami grupy kadra administracyjna i grupy studenci (różne kierunki) pod względem stopnia zagrożenia systemu uczelni wyższej przez obecność podejrzanego oprogramowania.

$$r_{xy} = \frac{\frac{1}{n}\sum_{i=1}^{n}(x_i-\bar{x})(y_i-\bar{y})}{S_x S_y}=0{,}74$$

$$\mathrm{WD}=r_{xy}^{2} * 100\% = 54{,}76\%$$

Wykres 3.66. Zależność między respondentami grupy kadry administracyjnej i grupy studenci (różne kierunki) pod względem stopnia zagrożenia systemu uczelni wyższej przez obecność podejrzanego oprogramowania



Źródło: opracowanie własne na podstawie badań własnych

W związku z faktem, że wartość liczbowa w ocenie relacji jest dodatnia oznacza to, iż wraz ze wzrostem wartości jednej zmiennej rosną wartości także drugiej.

13. Jak Państwo oceniają zagrożenia systemu informacyjnego w uczelni wyższej?

l) Manipulacja danymi w systemie

Rozkład odpowiedzi respondentów grupy nauczyciele akademiccy i kadra administracyjna dotyczący oceny przez użytkowników stopnia zagrożenia systemu uczelni wyższej przez manipulację danymi w systemie prezentuje tabela 3.34.

Tabela 3.34. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy kadra administracyjna na temat zagrożeń systemu informacyjnego w uczelni wyższej przez manipulację danymi w systemie

Odpowiedzi badanych osób manipulacja danymi w systemie						
Osoby poddane badaniu	**Respondenci nauczyciele akademiccy**		**Respondenci kadra administracyjna**		**OGÓŁEM**	
Ocena	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***
bardzo niska	69	13,8%	142	28,4%	211	21,1%
niska	346	69,2%	296	59,2%	642	64,2%
przeciętna	39	7,8%	29	5,8%	68	6,8%
wysoka	29	5,8%	28	5,6%	57	5,7%
bardzo wysoka	17	3,4%	5	1%	22	2,2%
	500	**100%**	**500**	**100%**	**1000**	**100%**

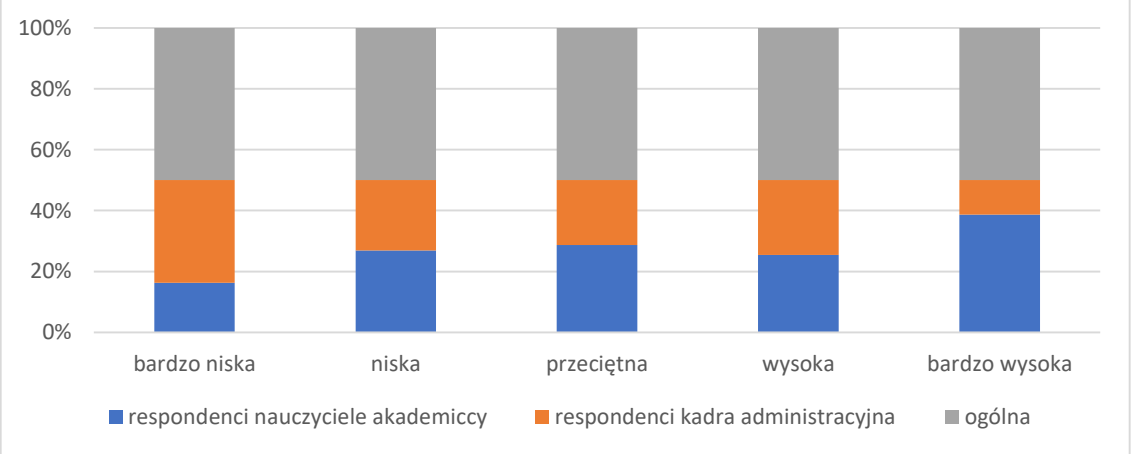
Źródło: opracowanie własne na podstawie badań własnych

W badaniu wzięło udział 500 osób zatrudnionych na stanowisku, nauczycieli akademickich oraz 500 osób zatrudnionych na stanowisku kadra administracyjna. Z przeprowadzonej analizy wynika, że nauczyciele akademiccy jak i kadra administracyjna ocenili stopień zagrożenia systemu uczelni wyższej przez manipulację danymi w systemie, jako niski. Wskazuje na to 346 respondentów, co w udziale procentowym wynosi 69,2% dla nauczycieli akademickich i 296 respondentów, co w udziale procentowym dla kadry administracyjnej wynosi 59,2%.

Analizując udzielone odpowiedzi w opinii 17 respondentów, co w udziale procentowym wynosi 3,4% dla nauczycieli akademickich i 5 respondentów, co w udziale procentowym daje 1% dla kadry administracyjnej świadczy, że pojawienie się manipulacji danymi w systemie stanowi bardzo duże zagrożenie dla systemu informacyjnego uczelni wyższej.

Wykres 3.67. przedstawia odpowiedzi respondentów grupy nauczyciele akademiccy i grupy kadra administracyjna na temat stopnia zagrożenia systemu uczelni wyższej przez manipulację danymi w systemie.

Wykres 3.67. ***Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy kadra administracyjna na temat stopnia zagrożenia systemu uczelni wyższej przez manipulację danymi w systemie***



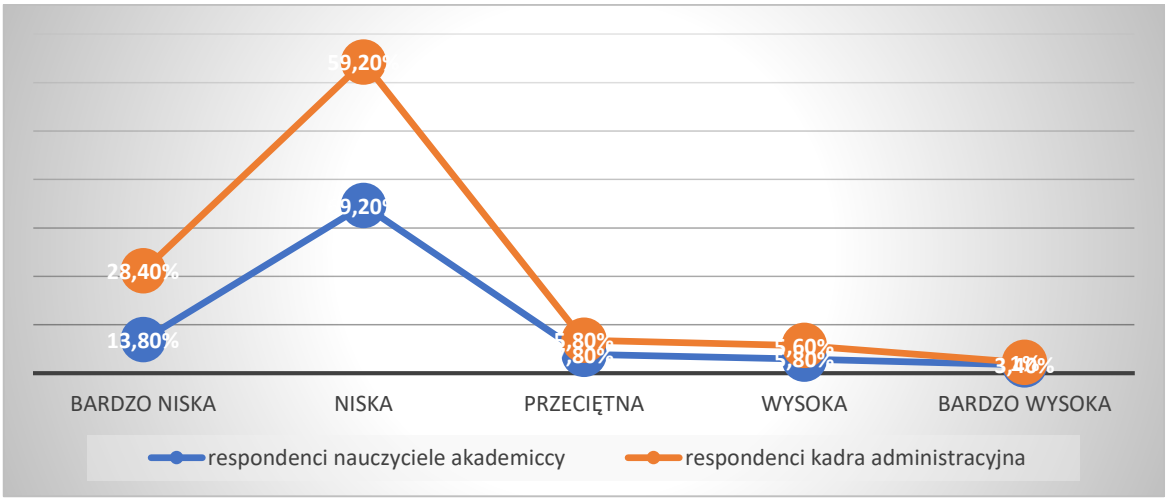
Źródło: opracowanie własne na podstawie badań własnych

O stopniu zależności świadczy współczynnik korelacji liniowej Pearsona na poziomie 0,95 i współczynnik determinacji liniowej, który wskazuje procent wyjaśnionej liniowo zmienności równy 90,25%. Wykres 3.68. pokazuje zależność między respondentami grupy nauczyciele akademiccy i grupy kadra administracyjna pod względem stopnia zagrożenia systemu uczelni wyższej przez manipulację danymi w systemie.

$$r_{xy} = \frac{\frac{1}{n}\sum_{i=1}^{n}(x_i-\bar{x})(y_i-\bar{y})}{S_x S_y}=0{,}95$$

$$WD=r\frac{2}{xy} * 100\% = 90{,}25\%$$

Wykres 3.68. Zależność między respondentami grupy nauczyciele akademiccy i grupy kadra administracyjna pod względem stopnia zagrożenia systemu uczelni wyższej przez manipulację danymi w systemie



Źródło: opracowanie własne na podstawie badań własnych

W związku z faktem, że wartość liczbowa w ocenie relacji jest dodatnia oznacza to, iż wraz ze wzrostem wartości jednej zmiennej rosną wartości także drugiej. Tabela 3.35. przedstawia odpowiedzi respondentów grupy nauczyciele akademiccy i grupy studenci (różne kierunki) na temat zagrożeń systemu informacyjnego w uczelni wyższej przez manipulację danymi w systemie.

Tabela 3.35. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy studenci (różne kierunki) na temat zagrożeń systemu informacyjnego w uczelni wyższej przez manipulację danymi w systemie

Odpowiedzi badanych osób manipulacja danymi w systemie						
Osoby poddane badaniu	**Respondenci nauczyciele akademiccy**		**Respondenci studenci (różne kierunki)**		**OGÓŁEM**	
Ocena	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***
bardzo niska	69	13,8%	59	11,8%	128	12,8%
niska	346	69,2%	268	53,6%	614	61,4%
przeciętna	39	7,8%	159	31,8%	198	19,8%
wysoka	29	5,8%	8	1,6%	37	3,7%
bardzo wysoka	17	3,4%	6	1,2%	23	2,3%
	500	**100%**	**500**	**100%**	**1000**	**100%**

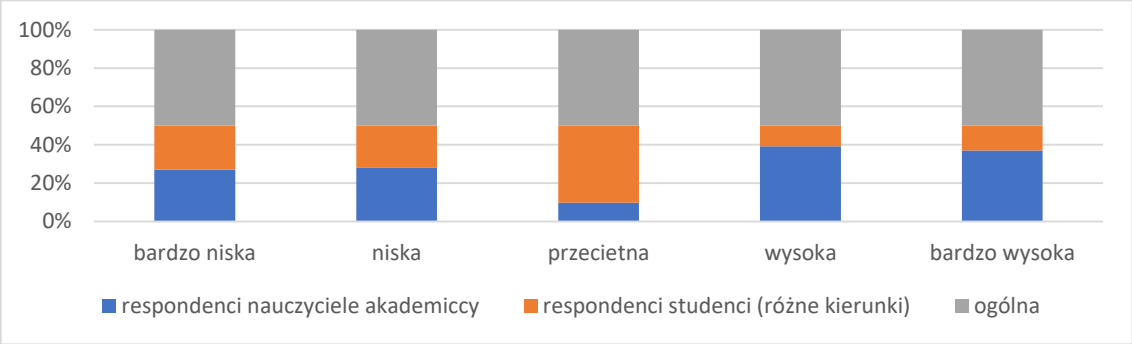
Źródło: opracowanie własne na podstawie badań własnych

W badaniu wzięło udział 500 osób zatrudnionych na stanowisku, nauczycieli akademickich oraz 500 osób studiujących w uczelni wyższej. Z przeprowadzonej analizy wynika, że nauczyciele akademiccy jak i studenci (różne kierunki) ocenili stopień zagrożenia systemu uczelni wyższej przez manipulację danymi w systemie, jako niski. Wskazuje na to 346 respondentów, co w udziale procentowym wynosi 69,2% dla nauczycieli akademickich i 268 respondentów, co w udziale procentowym dla studentów (różne roczniki) wynosi 53,6%.

Analizując udzielone odpowiedzi w opinii 17 respondentów, co w udziale procentowym wynosi 3,4% dla nauczycieli akademickich i 6 respondentów, co w udziale procentowym daje 1,2% dla studentów studiujących w uczelni wyższej świadczy, że pojawienie się manipulacji danymi w systemie stanowi bardzo duże zagrożenie dla systemu informacyjnego uczelni wyższej.

Wykres 3.69. przedstawia odpowiedzi respondentów grupy nauczyciele akademiccy i grupy studenci (różne kierunki) na temat stopnia zagrożenia systemu uczelni wyższej przez manipulację danymi w systemie.

Wykres 3.69. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy studenci (różne kierunki) na temat stopnia zagrożenia systemu uczelni wyższej przez manipulację danymi w systemie



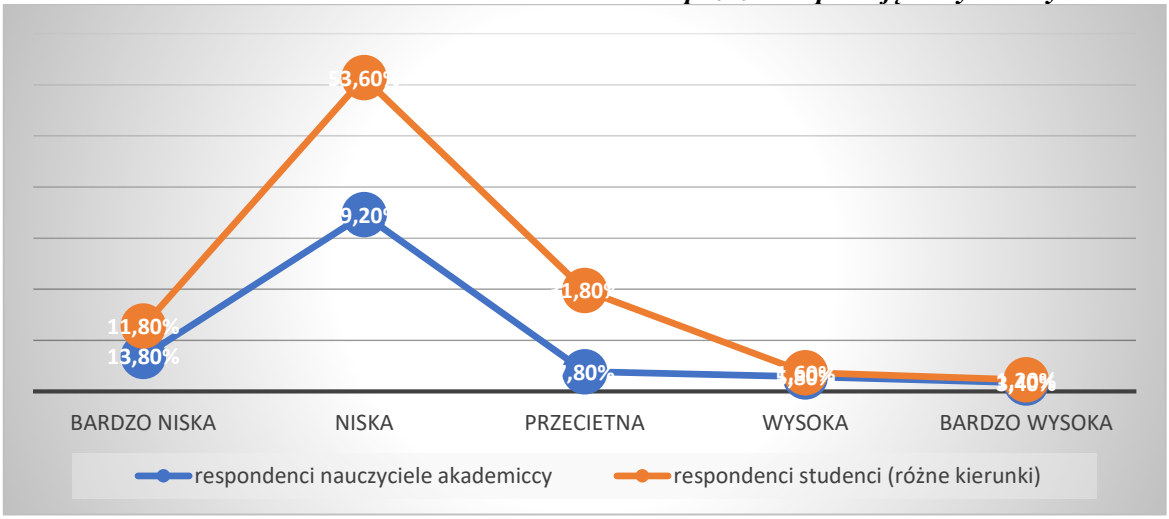
Źródło: opracowanie własne na podstawie badań własnych

O stopniu zależności świadczy współczynnik korelacji liniowej Pearsona na poziomie 0,85 i współczynnik determinacji liniowej, który wskazuje procent wyjaśnionej liniowo zmienności równy 72,25%. Wykres 3.70. pokazuje zależność między respondentami grupy nauczyciele akademiccy i grupy studenci (różne kierunki) pod względem stopnia zagrożenia systemu uczelni wyższej przez manipulację danymi w systemie.

$$r_{xy} = \frac{\frac{1}{n}\sum_{i=1}^{n}(x_i-\bar{x})(y_i-\bar{y})}{S_x S_y} = 0{,}85$$

$$WD=r\frac{2}{xy} * 100\% = 72{,}25\%$$

Wykres 3.70. Zależność między respondentami grupy nauczyciele akademiccy i grupy studenci (różne kierunki) pod względem stopnia zagrożenia systemu uczelni wyższej przez manipulację danymi w systemie



Źródło: opracowanie własne na podstawie badań własnych

W związku z faktem, że wartość liczbowa w ocenie relacji jest dodatnia oznacza to, iż wraz ze wzrostem wartości jednej zmiennej rosną wartości także drugiej. Tabela 3.36. przedstawia odpowiedzi respondentów grupy kadra administracyjna i grupy studenci (różne kierunki) na temat zagrożeń systemu informacyjnego w uczelni wyższej przez manipulację danymi w systemie.

Tabela 3.36. Odpowiedzi respondentów grupy kadra administracyjna i grupy studenci (różne kierunki) na temat zagrożeń systemu informacyjnego w uczelni wyższej przez manipulację danymi w systemie

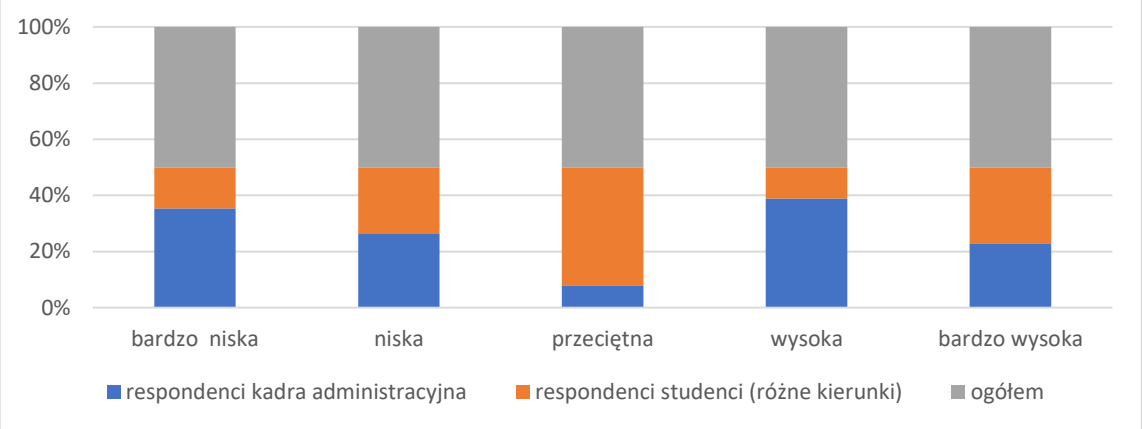
Odpowiedzi badanych osób manipulacja danymi w systemie						
Osoby poddane badaniu	**Respondenci kadra administracyjna**		**Respondenci studenci (różne kierunki)**		**OGÓŁEM**	
Ocena	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***
bardzo niska	142	28,4%	59	11,8%	201	20,1%
niska	296	59,2%	268	53,6%	564	56,4%
przeciętna	29	5,8%	159	31,8%	188	18,8%
wysoka	28	5,6%	8	1,6%	36	3,6%
bardzo wysoka	5	1%	6	1,2%	11	1,1%
	500	**100%**	**500**	**100%**	**1000**	**100%**

Źródło: opracowanie własne na podstawie badań własnych

W badaniu wzięło udział 500 osób zatrudnionych na stanowisku, kadra administracyjna oraz 500 osób studiujących w uczelni wyższej. Z przeprowadzonej analizy wynika, że kadra administracyjna jak i studenci (różne kierunki) ocenili stopień zagrożenia systemu uczelni wyższej przez manipulację danymi w systemie, jako niski. Wskazuje na to 296 respondentów, co w udziale procentowym wynosi 59,2% dla kadry administracyjnej i 268 respondentów, co w udziale procentowym dla studentów (różne roczniki) wynosi 53,6%.

Analizując udzielone odpowiedzi w opinii 5 respondentów, co w udziale procentowym wynosi 1% kadry administracyjnej i 6 respondentów, co w udziale procentowym daje 1,2% dla studentów studiujących w uczelni wyższej świadczy, że pojawienie się manipulacji danymi w systemie stanowi bardzo duże zagrożenie dla systemu informacyjnego uczelni wyższej. Wykres 3.71. przedstawia odpowiedzi respondentów grupy kadry administracyjnej i grupy studenci (różne kierunki) na temat stopnia zagrożenia systemu uczelni wyższej przez manipulację danymi w systemie.

Wykres 3.71. Odpowiedzi respondentów grupy kadra administracyjna i grupy studenci (różne kierunki) na temat stopnia zagrożenia systemu uczelni wyższej przez manipulację danymi w systemie



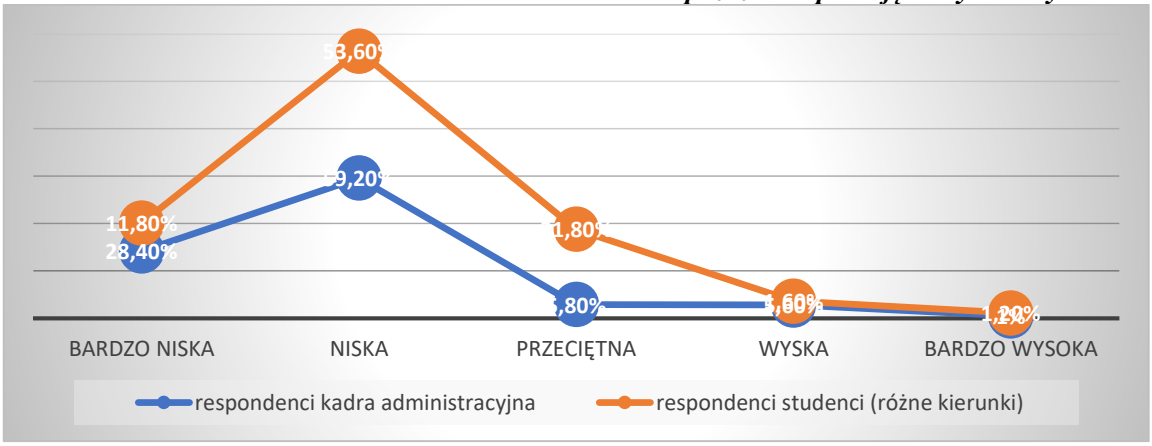
Źródło: opracowanie własne na podstawie badań własnych

O stopniu zależności świadczy współczynnik korelacji liniowej Pearsona na poziomie 0,78 i współczynnik determinacji liniowej, który wskazuje procent wyjaśnionej liniowo zmienności równy 60,84%. Wykres 3.72. pokazuje zależność między respondentami grupy kadra administracyjna i grupy studenci (różne kierunki) pod względem stopnia zagrożenia systemu uczelni wyższej przez manipulację danymi w systemie.

$$r_{xy} = \frac{\frac{1}{n}\sum_{i=1}^{n}(x_i-\bar{x})(y_i-\bar{y})}{S_x S_y}=0{,}78$$

$$WD=r\frac{2}{xy} * 100\% = 60{,}84\%$$

Wykres 3.72. Zależność między respondentami grupy kadra administracyjna i grupy studenci (różne kierunki) pod względem stopnia zagrożenia systemu uczelni wyższej przez manipulację danymi w systemie



Źródło: opracowanie własne na podstawie badań własnych

W związku z faktem, że wartość liczbowa w ocenie relacji jest dodatnia oznacza to, iż wraz ze wzrostem wartości jednej zmiennej rosną wartości także drugiej.

13. Jak Państwo oceniają zagrożenia systemu informacyjnego w uczelni wyższej?

m) Ujawnienie informacji podczas przesyłania

Rozkład odpowiedzi respondentów grupy nauczyciele akademiccy i kadra administracyjna dotyczący oceny przez użytkowników stopnia zagrożenia systemu uczelni wyższej przez ujawnienie informacji podczas przesyłania prezentuje tabela 3.37.

Tabela 3.37. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy kadra administracyjna na temat zagrożeń systemu informacyjnego w uczelni wyższej przez ujawnienie informacji podczas przesyłania

Odpowiedzi badanych osób ujawnienie informacji podczas przesyłania						
Osoby poddane badaniu	**Respondenci nauczyciele akademiccy**		**Respondenci kadra administracyjna**		**OGÓŁEM**	
Ocena	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***
bardzo niska	278	55,6%	119	23,8%	397	39,7%
niska	168	33,6%	238	47,6%	406	40,6%
przeciętna	26	5,2%	98	19,6%	124	12,4%
wysoka	18	3,6%	39	7,8%	57	5,7%
bardzo wysoka	10	2%	6	1,2%	16	1,6%
	500	**100%**	**500**	**100%**	**1000**	**100%**

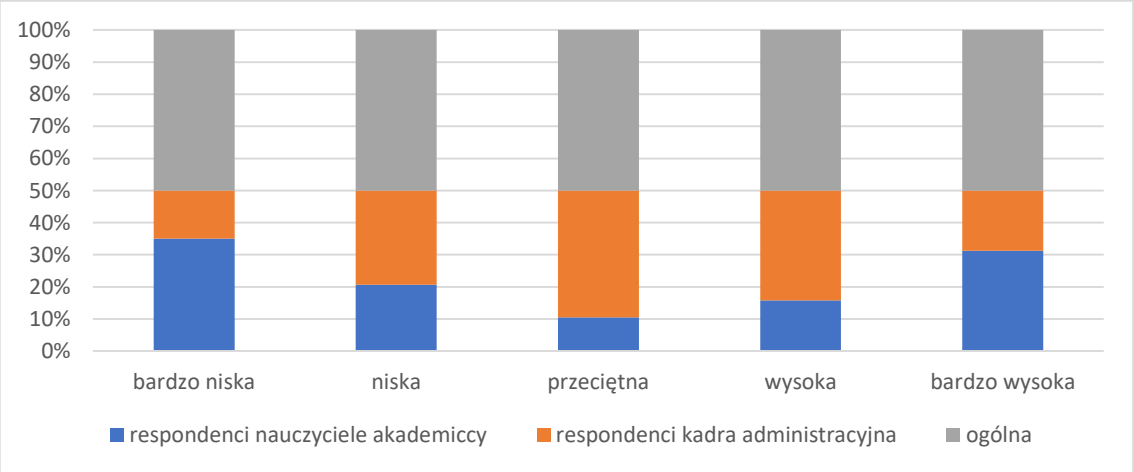
Źródło: opracowanie własne na podstawie badań własnych

W badaniu wzięło udział 500 osób zatrudnionych na stanowisku, nauczycieli akademickich oraz 500 osób zatrudnionych na stanowisku kadra administracyjna. Z przeprowadzonej analizy wynika, że nauczyciele akademiccy jak i kadra administracyjna ocenili stopień zagrożenia systemu uczelni wyższej przez ujawnienie informacji podczas przesyłania, jako bardzo niski i niski. Wskazuje na to 278 respondentów, co w udziale procentowym wynosi 55,6% dla nauczycieli akademickich i 238 respondentów, co w udziale procentowym dla kadry administracyjnej wynosi 47,6%.

Analizując udzielone odpowiedzi w opinii 10 respondentów, co w udziale procentowym wynosi 2% dla nauczycieli akademickich i 6 respondentów, co w udziale procentowym daje 1,2% dla kadry administracyjnej świadczy, że pojawienie się ujawnienia informacji podczas przesyłania stanowi bardzo duże zagrożenie dla systemu informacyjnego uczelni wyższej.

Wykres 3.73. przedstawia odpowiedzi respondentów grupy nauczyciele akademiccy i grupy kadra administracyjna na temat stopnia zagrożenia systemu uczelni wyższej przez ujawnienie informacji podczas przesyłania.

Wykres 3.73. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy kadra administracyjna na temat stopnia zagrożenia systemu uczelni wyższej przez ujawnienie informacji podczas przesyłania



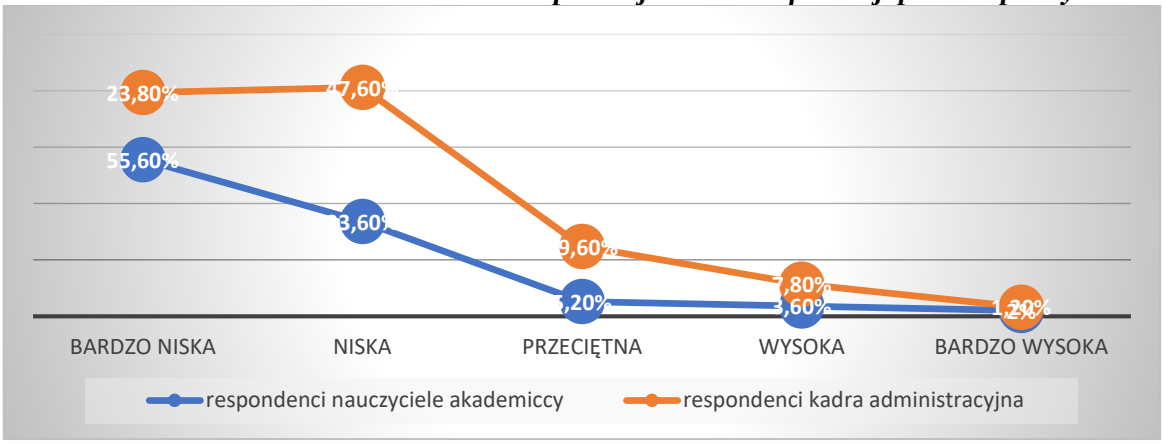
Źródło: opracowanie własne na podstawie badań własnych

O stopniu zależności świadczy współczynnik korelacji liniowej Pearsona na poziomie 0,62 i współczynnik determinacji liniowej, który wskazuje procent wyjaśnionej liniowo zmienności równy 38,44%. Wykres 3.74. pokazuje zależność między respondentami grupy nauczyciele akademiccy i grupy kadra administracyjna pod względem stopnia zagrożenia systemu uczelni wyższej przez ujawnienie informacji podczas przesyłania.

$$r_{xy} = \frac{\frac{1}{n}\sum_{i=1}^{n}(x_i-\bar{x})(y_i-\bar{y})}{S_x S_y}=0{,}62$$

$$WD=r\frac{2}{xy} * 100\% = 38{,}44\%$$

Wykres 3.74. Zależność między respondentami grupy nauczyciele akademiccy i grupy kadra administracyjna pod względem stopnia zagrożenia systemu uczelni wyższej przez ujawnienie informacji podczas przesyłania



Źródło: opracowanie własne na podstawie badań własnych

W związku z faktem, że wartość liczbowa w ocenie relacji jest dodatnia oznacza to, iż wraz ze wzrostem wartości jednej zmiennej rosną wartości także drugiej. Tabela 3.38. przedstawia odpowiedzi respondentów grupy nauczyciele akademiccy i grupy studenci (różne kierunki) na temat zagrożeń systemu informacyjnego w uczelni wyższej przez ujawnienie informacji podczas przesyłania

Tabela 3.38. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy studenci (różne kierunki) na temat zagrożeń systemu informacyjnego w uczelni wyższej przez ujawnienie informacji podczas przesyłania

Odpowiedzi badanych osób ujawnienie informacji podczas przesyłania						
Osoby poddane badaniu	**Respondenci nauczyciele akademiccy**		**Respondenci studenci (różne kierunki)**		**OGÓŁEM**	
Ocena	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***
bardzo niska	278	55,6%	169	33,8%	447	44,7%
niska	168	33,6%	289	57,8%	457	45,7%
przeciętna	26	5,2%	35	7%	61	6,1%
wysoka	18	3,6%	5	1%	23	2,3%
bardzo wysoka	10	2%	2	0,4%	12	1,2%
	500	**100%**	**500**	**100%**	**1000**	**100%**

Źródło: opracowanie własne na podstawie badań własnych

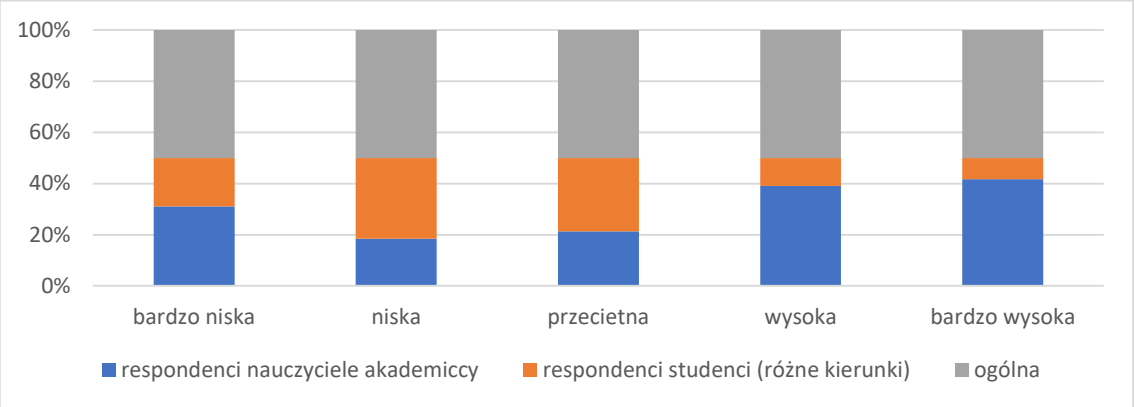
W badaniu wzięło udział 500 osób zatrudnionych na stanowisku, nauczycieli akademickich oraz 500 osób studiujących w uczelni wyższej. Z przeprowadzonej analizy

wynika, że nauczyciele akademiccy jak i studenci (różne kierunki) ocenili stopień zagrożenia systemu uczelni wyższej przez ujawnienie informacji podczas przesyłania, jako bardzo niski i niski. Wskazuje na to 278 respondentów, co w udziale procentowym wynosi 55,6% dla nauczycieli akademickich i 289 respondentów, co w udziale procentowym dla studentów (różne roczniki) wynosi 57,8%.

Analizując udzielone odpowiedzi w opinii 10 respondentów, co w udziale procentowym wynosi 2% dla nauczycieli akademickich i 2 respondentów, co w udziale procentowym daje 0,4% dla studentów studiujących w uczelni wyższej świadczy, że pojawienie się ujawnienia informacji podczas przesyłania stanowi bardzo duże zagrożenie dla systemu informacyjnego uczelni wyższej.

Wykres 3.75. przedstawia odpowiedzi respondentów grupy nauczyciele akademiccy i grupy studenci (różne kierunki) na temat stopnia zagrożenia systemu uczelni wyższej przez ujawnienie informacji podczas przesyłania.

Wykres 3.75. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy studenci (różne kierunki) na temat stopnia zagrożenia systemu uczelni wyższej przez ujawnienie informacji podczas przesyłania



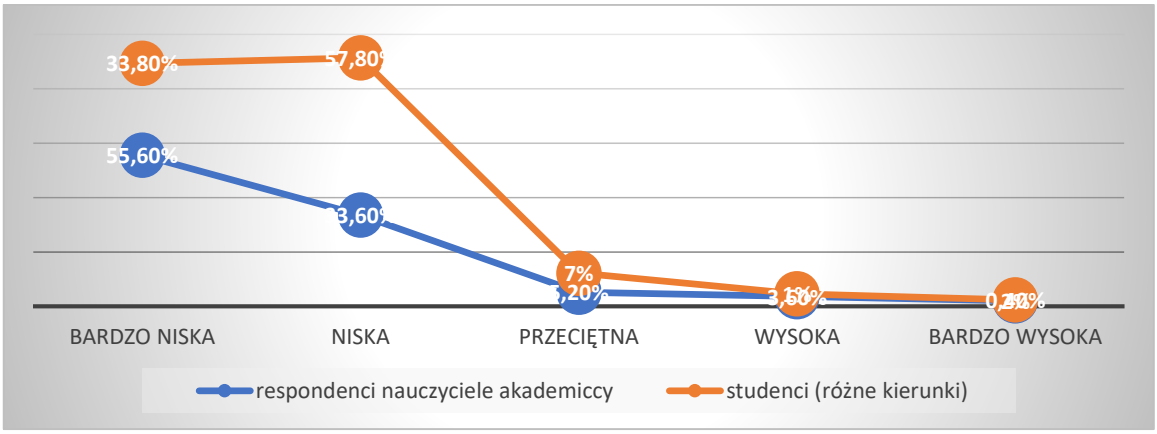
Źródło: opracowanie własne na podstawie badań własnych

O stopniu zależności świadczy współczynnik korelacji liniowej Pearsona na poziomie 0,78 i współczynnik determinacji liniowej, który wskazuje procent wyjaśnionej liniowo zmienności równy 60,84%. Wykres 3.76. pokazuje zależność między respondentami grupy nauczyciele akademiccy i grupy studenci (różne kierunki) pod względem stopnia zagrożenia systemu uczelni wyższej przez ujawnienie informacji podczas przesyłania.

$$r_{xy} = \frac{\frac{1}{n}\sum_{i=1}^{n}(x_i-\bar{x})(y_i-\bar{y})}{S_x S_y}=0{,}78$$

$$\mathrm{WD}=r\frac{2}{xy} * 100\% = 60{,}84\%$$

Wykres 3.76. Zależność między respondentami grupy nauczyciele akademiccy i grupy studenci (różne kierunki) pod względem stopnia zagrożenia systemu uczelni wyższej przez ujawnienie informacji podczas przesyłania



Źródło: opracowanie własne na podstawie badań własnych

W związku z faktem, że wartość liczbowa w ocenie relacji jest dodatnia oznacza to, iż wraz ze wzrostem wartości jednej zmiennej rosną wartości także drugiej. Tabela 3.39. przedstawia odpowiedzi respondentów grupy kadra administracyjna i grupy studenci (różne kierunki) na temat zagrożeń systemu informacyjnego w uczelni wyższej przez ujawnienie informacji podczas przesyłania.

Tabela 3.39. Odpowiedzi respondentów grupy kadra administracyjna i grupy studenci (różne kierunki) na temat zagrożeń systemu informacyjnego w uczelni wyższej przez ujawnienie informacji podczas przesyłania

Odpowiedzi badanych osób ujawnienie informacji podczas przesyłania						
Osoby poddane badaniu	**Respondenci kadra administracyjna**		**Respondenci studenci (różne kierunki)**		**OGÓŁEM**	
Ocena	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***
bardzo niska	119	23,8%	169	33,8%	288	28,8%
niska	238	47,6%	289	57,8%	527	52,7%
przeciętna	98	19,6%	35	7%	133	13,3%
wysoka	39	7,8%	5	1%	44	4,4%
bardzo wysoka	6	1,2%	2	0,4%	8	0,8%
	500	**100%**	**500**	**100%**	**1000**	**100%**

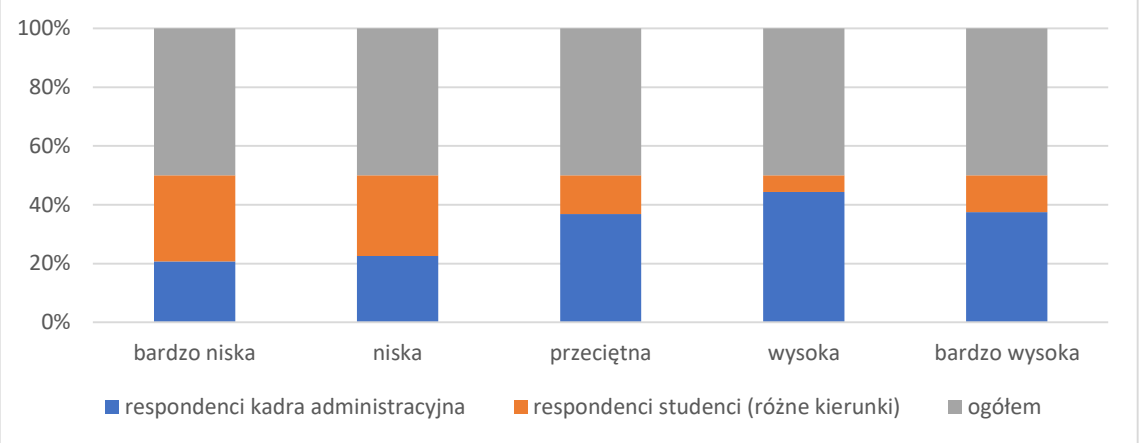
Źródło: opracowanie własne na podstawie badań własnych

W badaniu wzięło udział 500 osób zatrudnionych na stanowisku, kadry administracyjnej oraz 500 osób studiujących w uczelni wyższej. Z przeprowadzonej analizy wynika, że kadra administracyjna jak i studenci (różne kierunki) ocenili stopień zagrożenia

systemu uczelni wyższej przez ujawnienie informacji podczas przesyłania, jako niski. Wskazuje na to 238 respondentów, co w udziale procentowym wynosi 47,6% dla kadry administracyjnej i 289 respondentów, co w udziale procentowym dla studentów (różne roczniki) wynosi 57,8%.

Analizując udzielone odpowiedzi w opinii 6 respondentów, co w udziale procentowym wynosi 1,2% dla kadry administracyjnej i 2 respondentów, co w udziale procentowym daje 0,4% dla studentów studiujących w uczelni wyższej świadczy, że pojawienie się ujawnienia informacji podczas przesyłania stanowi bardzo duże zagrożenie dla systemu informacyjnego uczelni wyższej. Wykres 3.77. przedstawia odpowiedzi respondentów grupy kadry administracyjnej i grupy studentów (różne kierunki) na temat stopnia zagrożenia systemu uczelni wyższej przez ujawnienie informacji podczas przesyłania.

Wykres 3.77. Odpowiedzi respondentów grupy kadra administracyjna i grupy studenci (różne kierunki) na temat stopnia zagrożenia systemu uczelni wyższej przez ujawnienie informacji podczas przesyłania



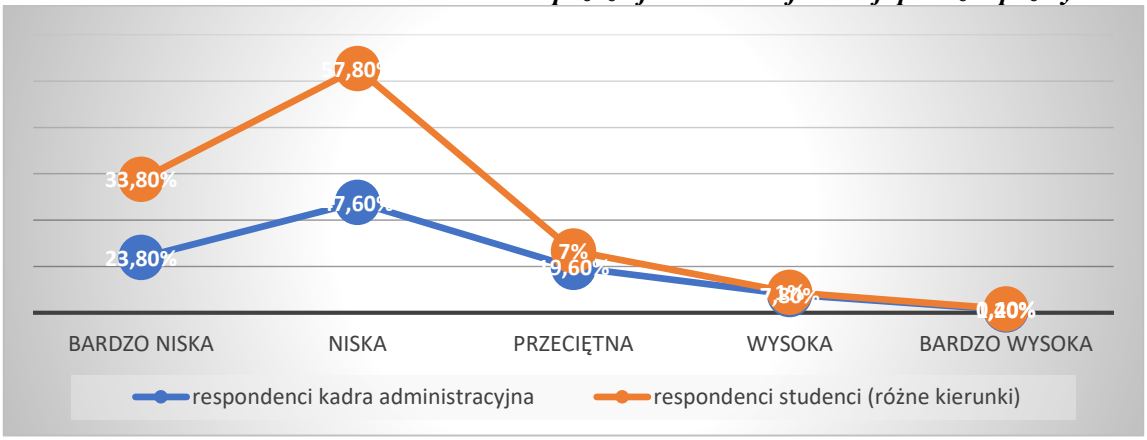
Źródło: opracowanie własne na podstawie badań własnych

O stopniu zależności świadczy współczynnik korelacji liniowej Pearsona na poziomie 0,94 i współczynnik determinacji liniowej, który wskazuje procent wyjaśnionej liniowo zmienności równy 88,36%. Wykres 3.78. pokazuje zależność między respondentami grupy kadra administracyjna i grupy studenci (różne kierunki) pod względem stopnia zagrożenia systemu uczelni wyższej przez ujawnienie informacji podczas przesyłania.

$$r_{xy} = \frac{\frac{1}{n}\sum_{i=1}^{n}(x_i-\bar{x})(y_i-\bar{y})}{S_x S_y}=0{,}94$$

$$\mathrm{WD}=r_{xy}^{2} * 100\% = 88{,}36\%$$

Wykres 3.78. Zależność między respondentami grupy kadra administracyjna i grupy studenci (różne kierunki) pod względem stopnia zagrożenia systemu uczelni wyższej przez ujawnienie informacji podczas przesyłania



Źródło: opracowanie własne na podstawie badań własnych

W związku z faktem, że wartość liczbowa w ocenie relacji jest dodatnia oznacza to, iż wraz ze wzrostem wartości jednej zmiennej rosną wartości także drugiej.

13. Jak Państwo oceniają zagrożenia systemu informacyjnego w uczelni wyższej?

n) Podszywanie się pod inną osobę

Rozkład odpowiedzi respondentów grupy nauczyciele akademiccy i kadra administracyjna dotyczący oceny przez użytkowników stopnia zagrożenia systemu uczelni wyższej przez podszywanie się pod inną osobę prezentuje tabela 3.40.

Tabela 3.40. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy kadra administracyjna na temat stopnia zagrożenia systemu uczelni wyższej przez podszywanie się pod inną osobę

Odpowiedzi badanych osób podszywanie się pod inną osobę						
Osoby poddane badaniu	**Respondenci nauczyciele akademiccy**		**Respondenci kadra administracyjna**		**OGÓŁEM**	
Ocena	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***
bardzo niska	312	62,4%	89	17,8%	401	40,1%
niska	89	17,8%	342	68,4%	431	43,1%
przeciętna	85	17%	49	9,8%	134	13,4%
wysoka	6	1,2%	17	34%	23	2,3%
bardzo wysoka	8	1,6%	3	0,6%	11	1,1%
	500	**100%**	**500**	**100%**	**1000**	**100%**

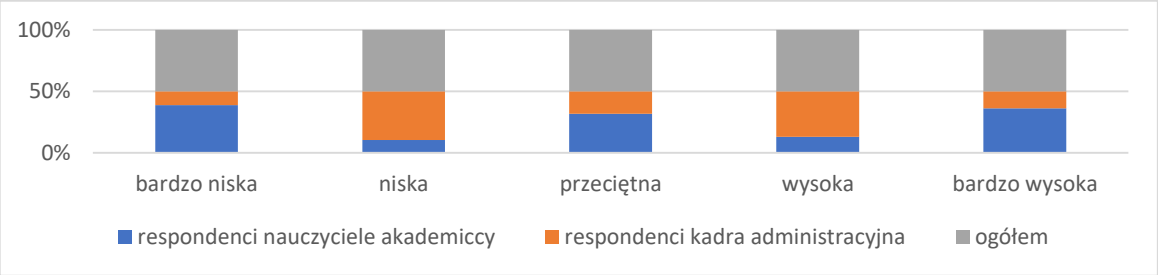
Źródło: opracowanie własne na podstawie badań własnych

W badaniu wzięło udział 500 osób zatrudnionych na stanowisku, nauczycieli akademickich oraz 500 osób zatrudnionych na stanowisku kadra administracyjna. Z przeprowadzonej analizy wynika, że nauczyciele akademiccy jak i kadra administracyjna ocenili stopień zagrożenia systemu uczelni wyższej przez podszywanie się pod inną osobę, jako bardzo niski i niski. Wskazuje na to 312 respondentów, co w udziale procentowym wynosi 62,4% dla nauczycieli akademickich i 342 respondentów, co w udziale procentowym dla kadry administracyjnej wynosi 68,4%.

Analizując udzielone odpowiedzi w opinii 8 respondentów, co w udziale procentowym wynosi 1,6% dla nauczycieli akademickich i 3 respondentów, co w udziale procentowym daje 0,6% dla kadry administracyjnej świadczy, że pojawienie się podszywania pod inną osobę stanowi bardzo duże zagrożenie dla systemu informacyjnego uczelni wyższej.

Wykres 3.79. przedstawia odpowiedzi respondentów grupy nauczyciele akademiccy i grupy kadra administracyjna na temat stopnia zagrożenia systemu uczelni wyższej przez podszywanie się pod inną osobę.

Wykres 3.79. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy kadra administracyjna na temat stopnia zagrożenia systemu uczelni wyższej przez podszywanie się pod inną osobę



Źródło: opracowanie własne na podstawie badań własnych

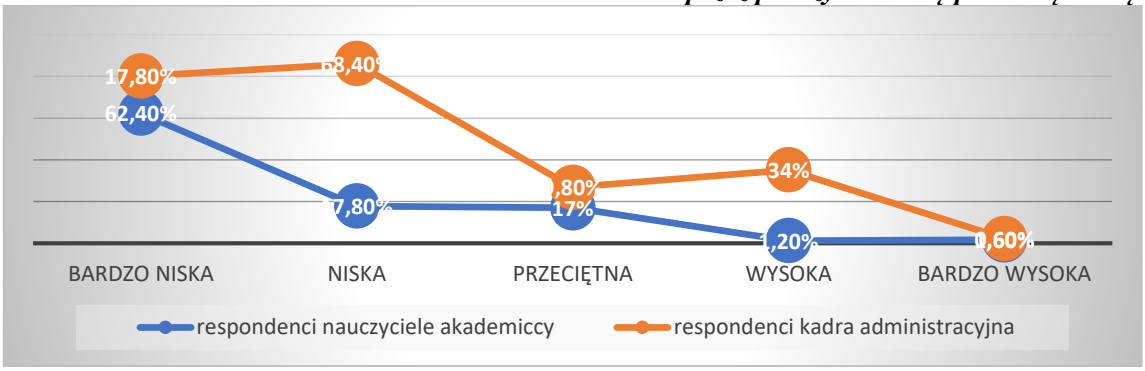
O stopniu zależności świadczy współczynnik korelacji liniowej Pearsona na poziomie 0,18 i współczynnik determinacji liniowej, który wskazuje procent wyjaśnionej liniowo zmienności równy 3,24%.

Wykres 3.80. pokazuje zależność między respondentami grupy nauczyciele akademiccy i grupy kadra administracyjna pod względem stopnia zagrożenia systemu uczelni wyższej przez podszywanie się pod inną osobę.

$$r_{xy} = \frac{\frac{1}{n}\sum_{i=1}^{n}(x_i-\bar{x})(y_i-\bar{y})}{S_x S_y}=0{,}18$$

$$\mathrm{WD}=r_{xy}^{2} * 100\% = 3{,}24\%$$

Wykres 3.80. Zależność między respondentami grupy nauczyciele akademiccy i grupy kadra administracyjna pod względem stopnia zagrożenia systemu uczelni wyższej przez podszywanie się pod inną osobę



Źródło: opracowanie własne na podstawie badań własnych

W związku z faktem, że wartość liczbowa w ocenie relacji jest dodatnia oznacza to, iż wraz ze wzrostem wartości jednej zmiennej rosną wartości także drugiej. Tabela 3.41. przedstawia odpowiedzi respondentów grupy nauczyciele akademiccy i grupy studenci (różne kierunki) na temat zagrożeń systemu informacyjnego w uczelni wyższej przez podszywanie się pod inną osobę.

Tabela 3.41. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy studentów (różne kierunki) na temat zagrożeń systemu informacyjnego w uczelni wyższej przez podszywanie się pod inną osobę

Odpowiedzi badanych osób podszywanie się pod inną osobę						
Osoby poddane badaniu	**Respondenci nauczyciele akademiccy**		**Respondenci studenci (różne kierunki)**		**OGÓŁEM**	
Ocena	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***
bardzo niska	312	62,4%	193	38,6%	505	50,5%
niska	89	17,8%	278	55,6%	367	36,7%
przeciętna	85	17%	18	3,6%	103	10,3%
wysoka	6	1,2%	6	1,2%	12	1,2%
bardzo wysoka	8	1,6%	5	1%	13	1,3%
	500	**100%**	**500**	**100%**	**1000**	**100%**

Źródło: opracowanie własne na podstawie badań własnych

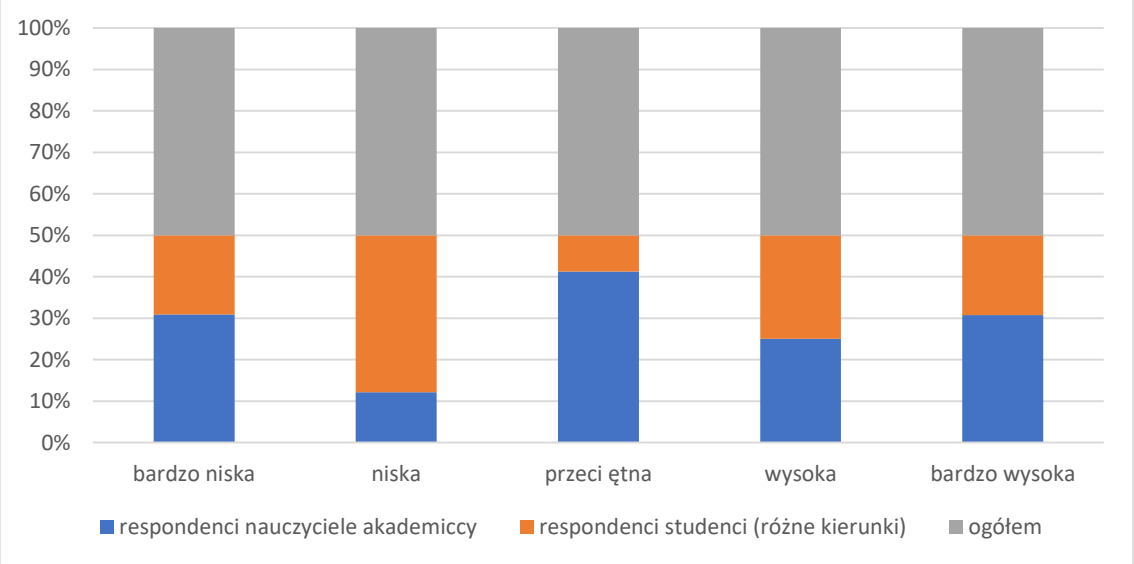
W badaniu wzięło udział 500 osób zatrudnionych na stanowisku, nauczycieli akademickich oraz 500 osób studiujących w uczelni wyższej. Z przeprowadzonej analizy wynika, że nauczyciele akademiccy jak i studenci (różne kierunki) ocenili stopień zagrożenia systemu uczelni wyższej przez podszywanie się pod inną osobę, jako bardzo niski i niski. Wskazuje na to 312 respondentów, co w udziale procentowym wynosi 62,4% dla

nauczycieli akademickich i 278 respondentów, co w udziale procentowym dla studentów (różne roczniki) wynosi 55,6%.

Analizując udzielone odpowiedzi w opinii 8 respondentów, co w udziale procentowym wynosi 1,6% dla nauczycieli akademickich i 5 respondentów, co w udziale procentowym daje 1% dla studentów studiujących w uczelni wyższej świadczy, że pojawienie się podszywania pod inną osobę stanowi bardzo duże zagrożenie dla systemu informacyjnego uczelni wyższej.

Wykres 3.81. przedstawia odpowiedzi respondentów grupy nauczyciele akademiccy i grupy studentów (różne kierunki) na temat stopnia zagrożenia systemu uczelni wyższej przez podszywanie się pod inną osobę.

Wykres 3.81. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy studenci (różne kierunki) na temat stopnia zagrożenia systemu uczelni wyższej przez podszywanie się pod inną osobę



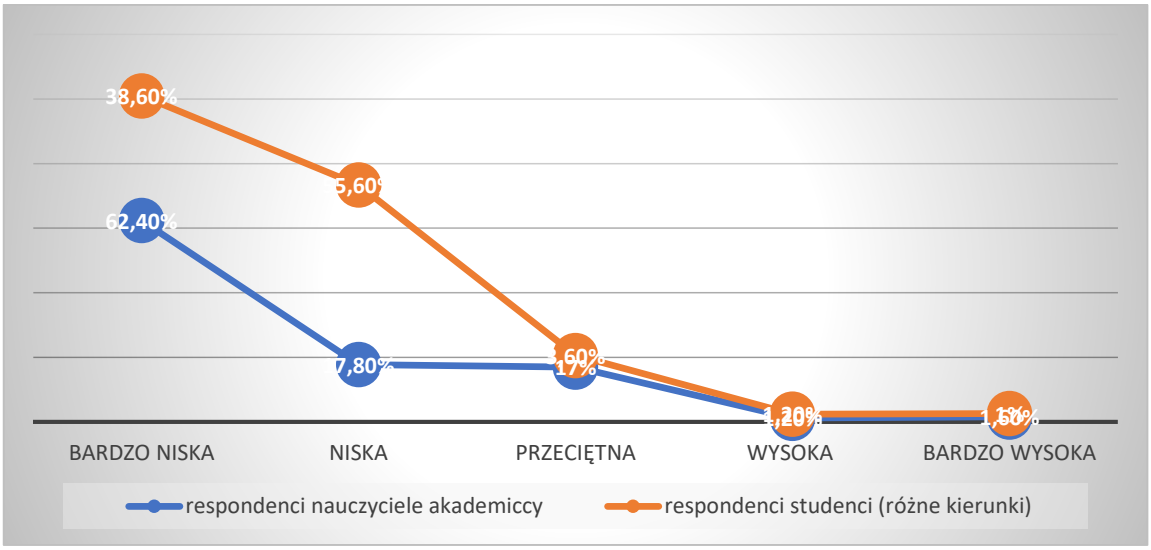
Źródło: opracowanie własne na podstawie badań własnych

O stopniu zależności świadczy współczynnik korelacji liniowej Pearsona na poziomie 0,57 i współczynnik determinacji liniowej, który wskazuje procent wyjaśnionej liniowo zmienności równy 32,49%. Wykres 3.82. pokazuje zależność między respondentami grupy nauczyciele akademiccy i grupy studenci (różne kierunki) pod względem stopnia zagrożenia systemu uczelni wyższej przez podszywanie się pod inną osobę.

$$r_{xy} = \frac{\frac{1}{n}\sum_{i=1}^{n}(x_i-\bar{x})(y_i-\bar{y})}{S_x S_y}=0{,}57$$

$$\mathrm{WD}=r\frac{2}{xy} * 100\% = 32{,}49\%$$

Wykres 3.82. Zależność między respondentami grupy nauczyciele akademiccy i grupy studenci (różne kierunki) pod względem stopnia zagrożenia systemu uczelni wyższej przez podszywanie się pod inną osobę



Źródło: opracowanie własne na podstawie badań własnych

W związku z faktem, że wartość liczbowa w ocenie relacji jest dodatnia oznacza to, iż wraz ze wzrostem wartości jednej zmiennej rosną wartości także drugiej. Tabela 3.42. przedstawia odpowiedzi respondentów grupy kadra administracyjna i grupy studenci (różne kierunki) na temat zagrożeń systemu informacyjnego w uczelni wyższej przez podszywanie się pod inną osobę.

Tabela 3.42. Odpowiedzi respondentów grupy kadra administracyjna i grupy studentów (różne kierunki) na temat zagrożeń systemu informacyjnego w uczelni wyższej przez podszywanie się pod inną osobę

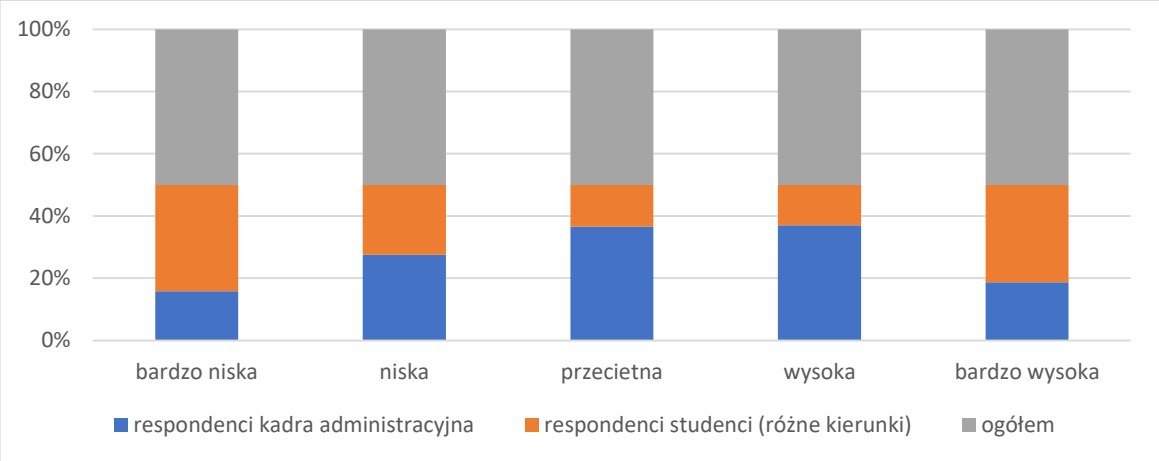
Odpowiedzi badanych osób podszywanie się pod inną osobę						
Osoby poddane badaniu	**Respondenci kadra administracyjna**		**Respondenci studenci (różne kierunki)**		**OGÓŁEM**	
Ocena	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***
bardzo niska	89	17,8%	193	38,6%	282	28,2%
niska	342	68,4%	278	55,6%	620	62%
przeciętna	49	9,8%	18	3,6%	67	6,7%
wysoka	17	34%	6	1,2%	23	2,3%
bardzo wysoka	3	0,6%	5	1%	8	0,8%
	500	**100%**	**500**	**100%**	**1000**	**100%**

Źródło: opracowanie własne na podstawie badań własnych

W badaniu wzięło udział 500 osób zatrudnionych na stanowisku, kadra administracyjna oraz 500 osób studiujących w uczelni wyższej. Z przeprowadzonej analizy wynika, że kadra administracyjna jak i studenci (różne kierunki) ocenili stopień zagrożenia systemu uczelni wyższej przez podszywanie się pod inną osobę, jako niski. Wskazuje na to 342 respondentów, co w udziale procentowym wynosi 68,4% dla kadry administracyjnej i 278 respondentów, co w udziale procentowym dla studentów (różne roczniki) wynosi 55,6%.

Analizując udzielone odpowiedzi w opinii 3 respondentów, co w udziale procentowym wynosi 0,6% dla kadry administracyjnej i 5 respondentów, co w udziale procentowym daje 1% dla studentów studiujących w uczelni wyższej świadczy, że pojawienie się podszywania pod inną osobę stanowi bardzo duże zagrożenie dla systemu informacyjnego uczelni wyższej. Wykres 3.83. przedstawia odpowiedzi respondentów grupy kadra administracyjna i grupy studenci (różne kierunki) na temat stopnia zagrożenia systemu uczelni wyższej przez podszywanie się pod inną osobę.

Wykres 3.83. Odpowiedzi respondentów grupy kadra administracyjna i grupy studenci (różne kierunki) na temat stopnia zagrożenia systemu uczelni wyższej przez podszywanie się pod inną osobę



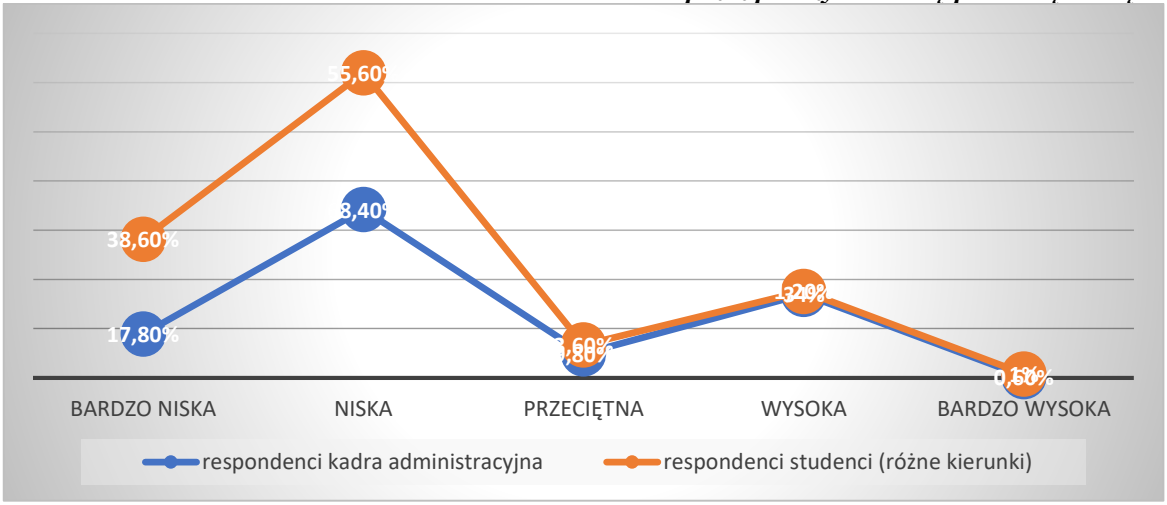
Źródło: opracowanie własne na podstawie badań własnych

O stopniu zależności świadczy współczynnik korelacji liniowej Pearsona na poziomie 0,89 i współczynnik determinacji liniowej, który wskazuje procent wyjaśnionej liniowo zmienności równy 79,21%. Wykres 3.84. pokazuje zależność między respondentami grupy kadra administracyjna i grupy studenci (różne kierunki) pod względem stopnia zagrożenia systemu uczelni wyższej przez podszywanie się pod inną osobę.

$$r_{xy} = \frac{\frac{1}{n}\sum_{i=1}^{n}(x_i-\bar{x})(y_i-\bar{y})}{S_x S_y}=0{,}89$$

$$WD=r\frac{2}{xy} * 100\% = 79{,}21\%$$

Wykres 3.84. Zależność między respondentami grupy kadra administracyjna i grupy studenci (różne kierunki) pod względem stopnia zagrożenia systemu uczelni wyższej przez podszywanie się pod inną osobę



Źródło: opracowanie własne na podstawie badań własnych

W związku z faktem, że wartość liczbowa w ocenie relacji jest dodatnia oznacza to, iż wraz ze wzrostem wartości jednej zmiennej rosną wartości także drugiej.

13. Jak Państwo oceniają zagrożenia systemu informacyjnego w uczelni wyższej?

o) Błędy, wady oprogramowania

Rozkład odpowiedzi respondentów grupy nauczyciele akademiccy i grupy kadra administracyjna dotyczący oceny przez użytkowników stopnia zagrożenia systemu uczelni wyższej przez błędy, wady oprogramowania prezentuje tabela 3.43.

Tabela 3.43. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy kadra administracyjna na temat zagrożeń systemu informacyjnego w uczelni wyższej przez błędy, wady oprogramowania

Odpowiedzi badanych osób błędy, wady oprogramowania						
Osoby poddane badaniu	**Respondenci nauczyciele akademiccy**		**Respondenci kadra administracyjna**		**OGÓŁEM**	
Ocena	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***
bardzo niska	89	17,8%	46	9,2%	135	13,5%
niska	99	19,8%	389	77,8%	488	48,8%
przeciętna	259	51,8%	28	5,6%	287	28,7%
wysoka	49	9,8%	30	6%	79	7,9%
bardzo wysoka	4	0,8%	7	1,4%	11	1,1%
	500	**100%**	**500**	**100%**	**1000**	**100%**

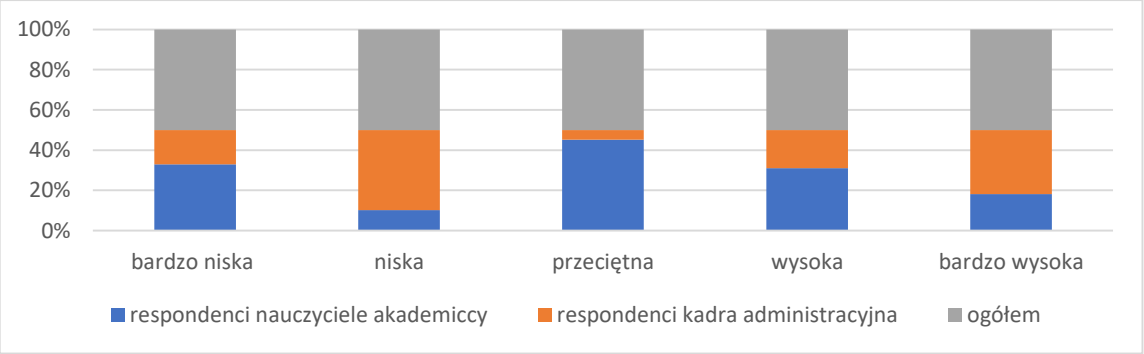
Źródło: opracowanie własne na podstawie badań własnych

W badaniu wzięło udział 500 osób zatrudnionych na stanowisku, nauczycieli akademickich oraz 500 osób zatrudnionych na stanowisku kadry administracyjnej. Z przeprowadzonej analizy wynika, że nauczyciele akademiccy jak i kadra administracyjna ocenili stopień zagrożenia systemu uczelni wyższej przez błędy, wady oprogramowania, jako przeciętny i niski. Wskazuje na to 259 respondentów, co w udziale procentowym wynosi 51,8% dla nauczycieli akademickich i 389 respondentów, co w udziale procentowym dla kadry administracyjnej wynosi 77,8%.

Analizując udzielone odpowiedzi w opinii 4 respondentów, co w udziale procentowym wynosi 0,8% dla nauczycieli akademickich i 7 respondentów, co w udziale procentowym daje 1,4% dla kadry administracyjnej świadczy, że pojawienie się błędów, wad oprogramowania stanowi bardzo duże zagrożenie dla systemu informacyjnego uczelni wyższej.

Wykres 3.85. przedstawia odpowiedzi respondentów grupy nauczyciele akademiccy i grupy kadra administracyjna na temat stopnia zagrożenia systemu uczelni wyższej przez błędy, wady oprogramowania.

Wykres 3.85. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy kadra administracyjna na temat stopnia zagrożenia systemu uczelni wyższej przez błędy, wady oprogramowania



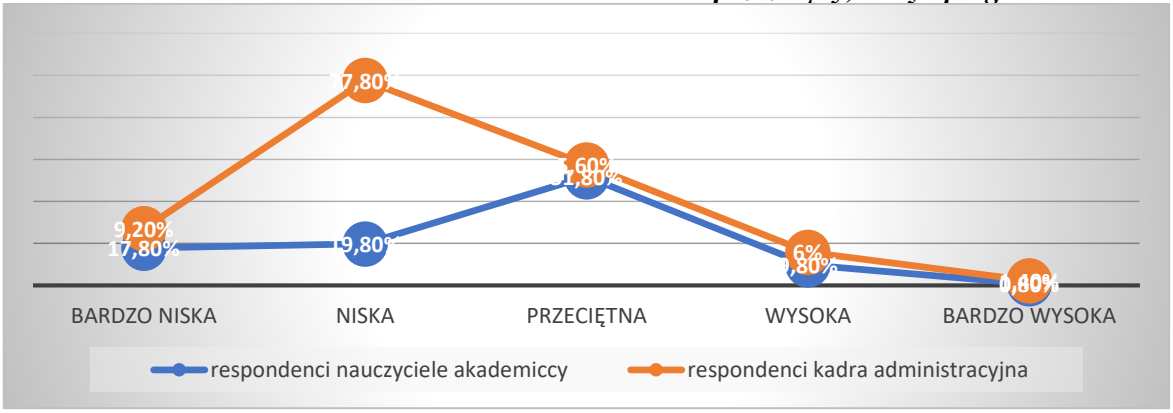
Źródło: opracowanie własne na podstawie badań własnych

O stopniu zależności świadczy współczynnik korelacji liniowej Pearsona na poziomie 0,02 i współczynnik determinacji liniowej, który wskazuje procent wyjaśnionej liniowo zmienności równy 4%. Wykres 3.86. pokazuje zależność między respondentami grupy nauczyciele akademiccy i grupy kadra administracyjna pod względem stopnia zagrożenia systemu uczelni wyższej przez błędy, wady oprogramowania.

$$r_{xy} = \frac{\frac{1}{n}\sum_{i=1}^{n}(x_i-\bar{x})(y_i-\bar{y})}{S_x S_y}=0{,}02$$

$$WD=r\frac{2}{xy} * 100\% = 4\%$$

Wykres 3.86. Zależność między respondentami grupy nauczyciele akademiccy i grupy kadra administracyjna pod względem stopnia zagrożenia systemu uczelni wyższej przez błędy, wady oprogramowania



Źródło: opracowanie własne na podstawie badań własnych

W związku z faktem, że wartość liczbowa w ocenie relacji jest dodatnia oznacza to, iż wraz ze wzrostem wartości jednej zmiennej rosną wartości także drugiej. Tabela 3.44. przedstawia odpowiedzi respondentów grupy nauczyciele akademiccy i grupy studenci (różne kierunki) na temat zagrożeń systemu informacyjnego w uczelni wyższej przez błędy, wady oprogramowania.

Tabela 3.44. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy studenci (różne kierunki) na temat zagrożeń systemu informacyjnego w uczelni wyższej przez błędy, wady oprogramowania

Odpowiedzi badanych osób błędy, wady oprogramowania						
Osoby poddane badaniu	**Respondenci nauczyciele akademiccy**		**Respondenci studenci (różne kierunki)**		**OGÓŁEM**	
Ocena	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***
bardzo niska	89	17,8%	198	39,6%	287	28,7%
niska	99	19,8%	158	31,6%	267	26,7%
przeciętna	259	51,8%	129	25,8%	388	38,8%
wysoka	49	9,8%	12	2,4%	61	6,1%
bardzo wysoka	4	0,8%	3	0,6%	7	0,7%
	500	**100%**	**500**	**100%**	**1000**	**100%**

Źródło: opracowanie własne na podstawie badań własnych

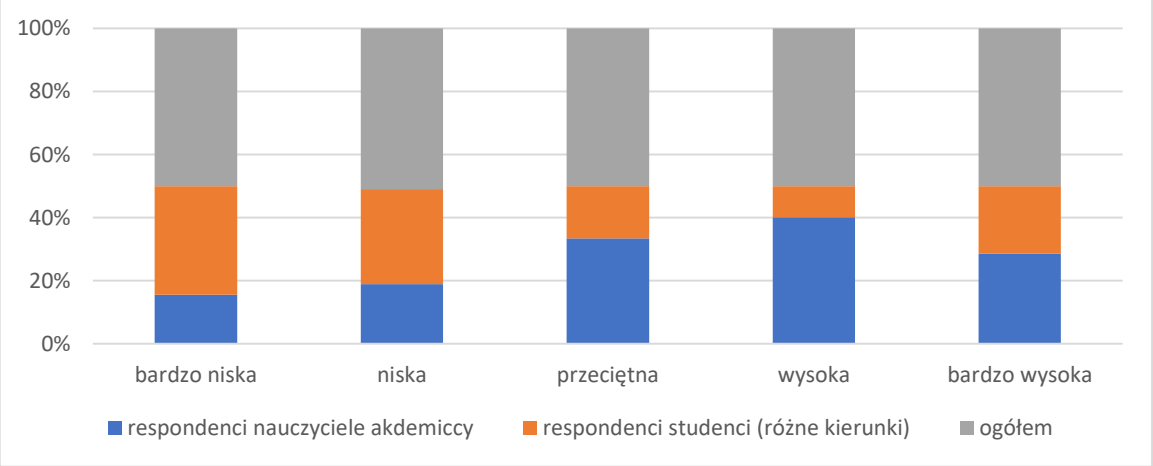
W badaniu wzięło udział 500 osób zatrudnionych na stanowisku, nauczycieli akademickich oraz 500 osób studiujących w uczelni wyższej. Z przeprowadzonej analizy wynika, że nauczyciele akademiccy jak i studenci (różne kierunki) ocenili stopień zagro-

żenia systemu uczelni wyższej przez błędy, wady oprogramowania, jako przeciętny i bardzo niski. Wskazuje na to 259 respondentów, co w udziale procentowym wynosi 51,8% dla nauczycieli akademickich i 198 respondentów, co w udziale procentowym dla studentów (różne roczniki) wynosi 39,6%.

Analizując udzielone odpowiedzi w opinii 4 respondentów, co w udziale procentowym wynosi 0,8% dla nauczycieli akademickich i 3 respondentów, co w udziale procentowym daje 0,6% dla studentów studiujących w uczelni wyższej świadczy, że pojawienie się błędów, wad oprogramowania stanowi bardzo duże zagrożenie dla systemu informacyjnego uczelni wyższej.

Wykres 3.87. przedstawia odpowiedzi respondentów grupy nauczyciele akademiccy i grupy studentów (różne kierunki) na temat stopnia zagrożenia systemu uczelni wyższej przez błędy, wady oprogramowania.

Wykres 3.87. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy studenci (różne kierunki) na temat stopnia zagrożenia systemu uczelni wyższej przez błędy, wady oprogramowania



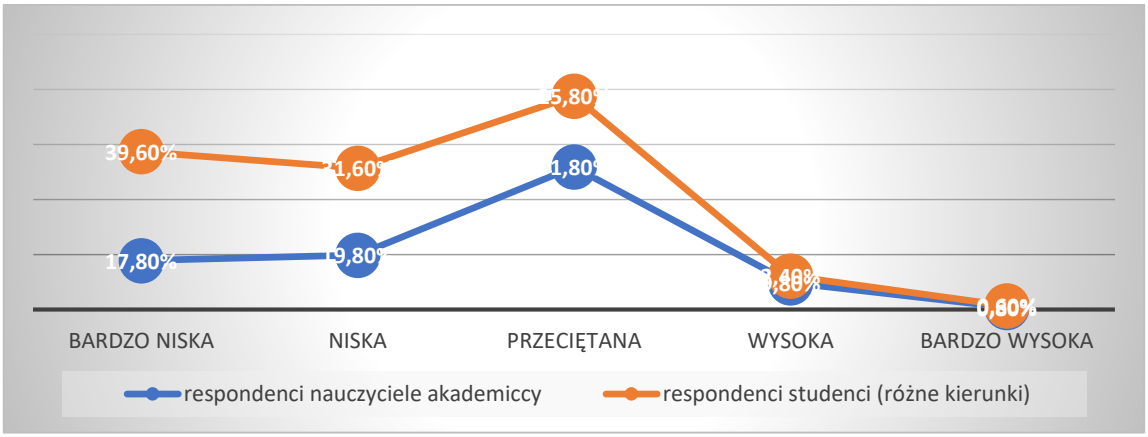
Źródło: opracowanie własne na podstawie badań własnych

O stopniu zależności świadczy współczynnik korelacji liniowej Pearsona na poziomie 0,51 i współczynnik determinacji liniowej, który wskazuje procent wyjaśnionej liniowo zmienności równy 26,01%. Wykres 3.88. pokazuje zależność między respondentami grupy nauczyciele akademiccy i grupy studenci (różne kierunki) pod względem stopnia zagrożenia systemu uczelni wyższej przez błędy, wady oprogramowania.

$$r_{xy} = \frac{\frac{1}{n}\sum_{i=1}^{n}(x_i-\bar{x})(y_i-\bar{y})}{S_x S_y}=0{,}51$$

$$\mathrm{WD}=r_{xy}^{2} * 100\% = 26{,}01\%$$

Wykres 3.88. Zależność między respondentami grupy nauczyciele akademiccy i grupy studenci (różne kierunki) pod względem stopnia zagrożenia systemu uczelni wyższej przez błędy, wady oprogramowania



Źródło: opracowanie własne na podstawie badań własnych

W związku z faktem, że wartość liczbowa w ocenie relacji jest dodatnia oznacza to, iż wraz ze wzrostem wartości jednej zmiennej rosną wartości także drugiej. Tabela 3.45. przedstawia odpowiedzi respondentów grupy kadra administracyjna i grupy studenci (różne kierunki) na temat zagrożeń systemu informacyjnego w uczelni wyższej przez błędy, wady oprogramowania.

Tabela 3.45. Odpowiedzi respondentów grupy kadra administracyjna i grupy studenci (różne kierunki) na temat zagrożeń systemu informacyjnego w uczelni wyższej przez błędy, wady oprogramowania

Odpowiedzi badanych osób błędy, wady oprogramowania						
Osoby poddane badaniu	**Respondenci kadra administracyjna**		**Respondenci studenci (różne kierunki)**		**OGÓŁEM**	
Ocena	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***
bardzo niska	46	9,2%	198	39,6%	244	24,4%
niska	389	77,8%	158	31,6%	547	54,7%
przeciętna	28	5,6%	129	25,8%	157	15,7%
wysoka	30	6%	12	2,4%	42	4,2%
bardzo wysoka	7	1,4%	3	0,6%	10	1%
	500	**100%**	**500**	**100%**	**1000**	**100%**

Źródło: opracowanie własne na podstawie badań własnych

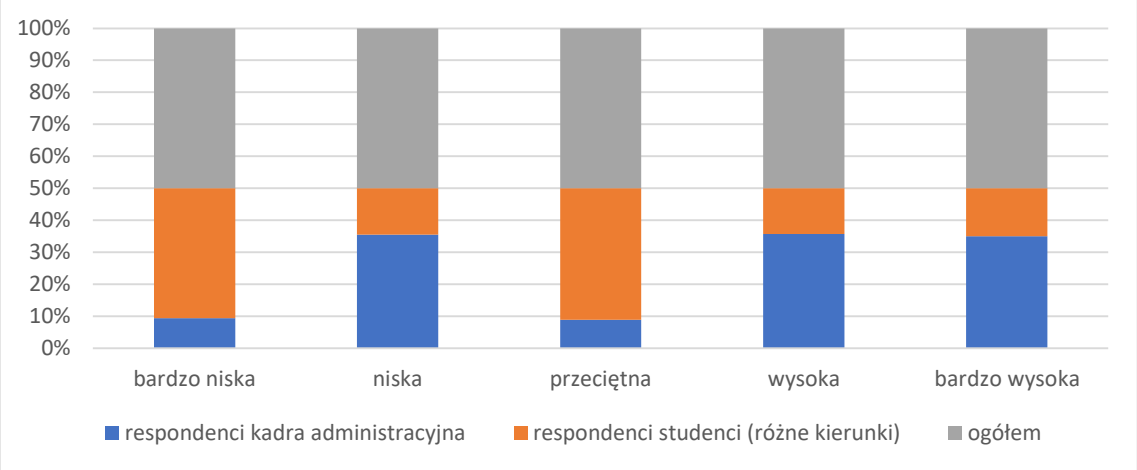
W badaniu wzięło udział 500 osób zatrudnionych na stanowisku, kadra administracyjna oraz 500 osób studiujących w uczelni wyższej. Z przeprowadzonej analizy wynika, że kadra administracyjna jak i studenci (różne kierunki) ocenili stopień zagrożenia systemu uczelni wyższej przez błędy, wady oprogramowania, jako niski i bardzo niski.

Wskazuje na to 389 respondentów, co w udziale procentowym wynosi 77,8% dla kadry administracyjnej i 198 respondentów, co w udziale procentowym dla studentów (różne roczniki) wynosi 39,6%.

Analizując udzielone odpowiedzi w opinii 7 respondentów, co w udziale procentowym wynosi 1,4% dla kadry administracyjnej i 3 respondentów, co w udziale procentowym daje 0,6% dla studentów studiujących w uczelni wyższej świadczy, że pojawienie się błędy, wady oprogramowania stanowi bardzo duże zagrożenie dla systemu informacyjnego uczelni wyższej.

Wykres 3.89. przedstawia odpowiedzi respondentów grupy kadra administracyjna i grupy studenci (różne kierunki) na temat stopnia zagrożenia systemu uczelni wyższej przez błędy, wady oprogramowania.

Wykres 3.89. Odpowiedzi respondentów grupy kadra administracyjna i grupy studenci (różne kierunki) na temat stopnia zagrożenia systemu uczelni wyższej przez błędy, wady oprogramowania



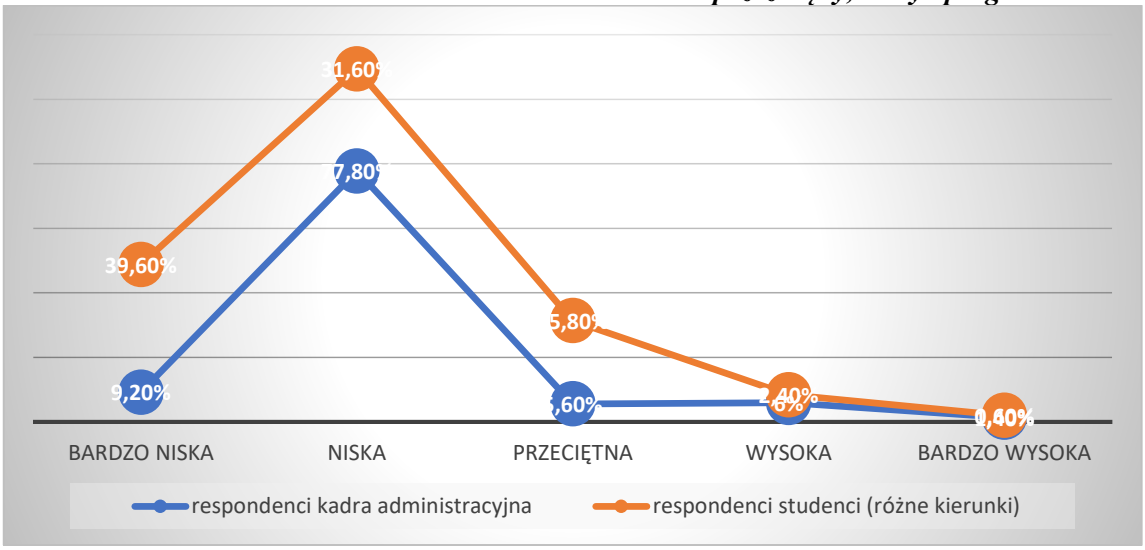
Źródło: opracowanie własne na podstawie badań własnych

O stopniu zależności świadczy współczynnik korelacji liniowej Pearsona na poziomie 0,43 i współczynnik determinacji liniowej, który wskazuje procent wyjaśnionej liniowo zmienności równy 18,49%. Wykres 3.90. pokazuje zależność między respondentami grupy kadra administracyjna i grupy studenci (różne kierunki) pod względem stopnia zagrożenia systemu uczelni wyższej przez błędy, wady oprogramowania.

$$r_{xy} = \frac{\frac{1}{n}\sum_{i=1}^{n}(x_i-\bar{x})(y_i-\bar{y})}{S_x S_y}=0{,}43$$

$$\mathrm{WD}=\mathrm{r}\frac{2}{xy} * 100\% = 18{,}49\%$$

Wykres 3.90. Zależność między respondentami grupy kadra administracyjna i grupy studenci (różne kierunki) pod względem stopnia zagrożenia systemu uczelni wyższej przez błędy, wady oprogramowania



Źródło: opracowanie własne na podstawie badań własnych

W związku z faktem, że wartość liczbowa w ocenie relacji jest dodatnia oznacza to, iż wraz ze wzrostem wartości jednej zmiennej rosną wartości także drugiej.

13. Jak Państwo oceniają zagrożenia systemu informacyjnego w uczelni wyższej?

p) Awarie sprzętowe i oprogramowania

Rozkład odpowiedzi respondentów grupy nauczyciele akademiccy i kadra administracyjna dotyczący oceny przez użytkowników stopnia zagrożenia systemu uczelni wyższej przez awarie sprzętowe i oprogramowania prezentuje tabela 3.46.

Tabela 3.46. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy kadra administracyjna na temat zagrożeń systemu informacyjnego w uczelni wyższej przez awarie sprzętowe i oprogramowania

Odpowiedzi badanych osób awarie sprzętowe i oprogramowania						
Osoby poddane badaniu	**Respondenci nauczyciele akademiccy**		**Respondenci kadra administracyjna**		**OGÓŁEM**	
Ocena	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***
bardzo niska	189	37,8%	139	27,8%	328	32,8%
niska	172	34,4%	169	33,8%	341	34,1%
przeciętna	122	24,4%	182	36,4%	304	30,4%
wysoka	15	3%	9	1,8%	24	2,4%
bardzo wysoka	2	0,4%	1	0,2%	3	0,3%
	500	**100%**	**500**	**100%**	**1000**	**100%**

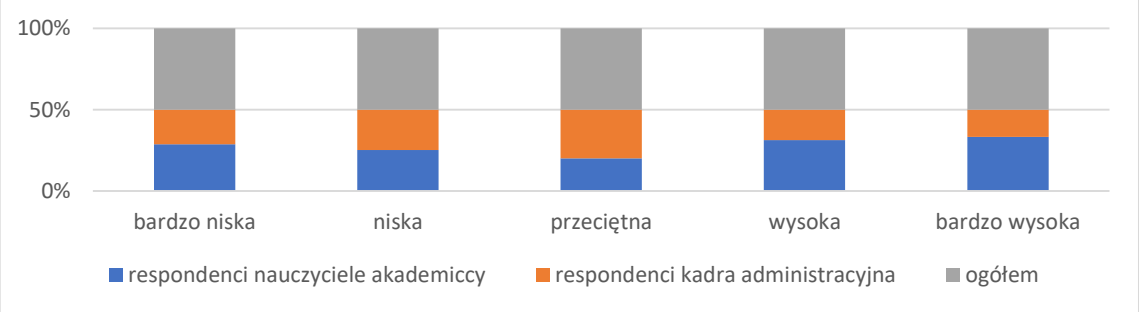
Źródło: opracowanie własne na podstawie badań własnych

W badaniu wzięło udział 500 osób zatrudnionych na stanowisku, nauczycieli akademickich oraz 500 osób zatrudnionych na stanowisku kadra administracyjna. Z przeprowadzonej analizy wynika, że nauczyciele akademiccy jak i kadra administracyjna ocenili stopień zagrożenia systemu uczelni wyższej przez awarie sprzętowe i oprogramowania, jako bardzo niski i przeciętny. Wskazuje na to 189 respondentów, co w udziale procentowym wynosi 37,8% dla nauczycieli akademickich i 182 respondentów, co w udziale procentowym dla kadry administracyjnej wynosi 36,4%.

Analizując udzielone odpowiedzi w opinii 2 respondentów, co w udziale procentowym wynosi 0,4% dla nauczycieli akademickich i 1 respondent, co w udziale procentowym daje 0,2% dla kadry administracyjnej świadczy, że pojawienie się awarii sprzętowych i oprogramowania stanowi bardzo duże zagrożenie dla systemu informacyjnego uczelni wyższej.

Wykres 3.91. przedstawia odpowiedzi respondentów grupy nauczyciele akademiccy i grupy kadra administracyjna na temat stopnia zagrożenia systemu uczelni wyższej przez awarie sprzętowe i oprogramowania.

Wykres 3.91. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy kadra administracyjna na temat stopnia zagrożenia systemu uczelni wyższej przez awarie sprzętowe i oprogramowania



Źródło: opracowanie własne na podstawie badań własnych

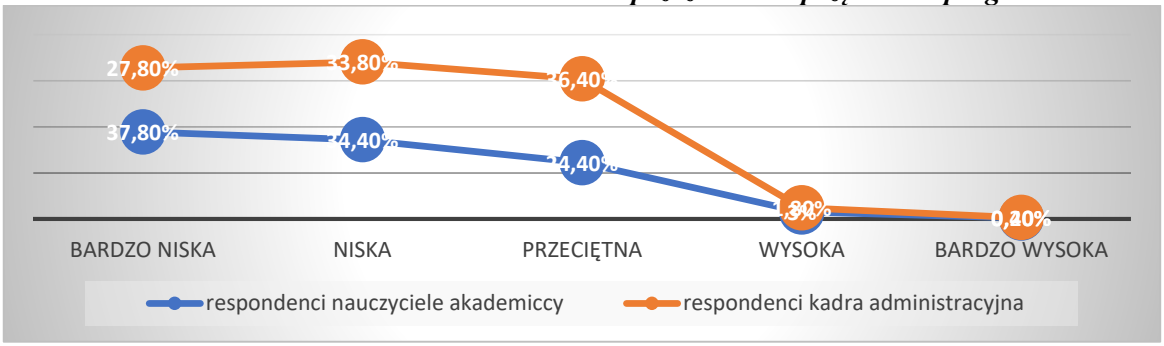
O stopniu zależności świadczy współczynnik korelacji liniowej Pearsona na poziomie 0,90 i współczynnik determinacji liniowej, który wskazuje procent wyjaśnionej liniowo zmienności równy 81%.

Wykres 3.92. pokazuje zależność między respondentami grupy nauczyciele akademiccy i grupy kadra administracyjna pod względem stopnia zagrożenia systemu uczelni wyższej przez awarie sprzętowe i oprogramowania.

$$r_{xy} = \frac{\frac{1}{n}\sum_{i=1}^{n}(x_i-\bar{x})(y_i-\bar{y})}{S_x S_y}=0{,}90$$

$$\mathrm{WD}=r_{xy}^{2} * 100\% = 81\%$$

Wykres 3.92. Zależność między respondentami grupy nauczyciele akademiccy i kadra administracyjna pod względem stopnia zagrożenia systemu uczelni wyższej przez awarie sprzętowe i oprogramowania



Źródło: opracowanie własne na podstawie badań własnych

W związku z faktem, że wartość liczbowa w ocenie relacji jest dodatnia oznacza to, iż wraz ze wzrostem wartości jednej zmiennej rosną wartości także drugiej. Tabela 3.47. przedstawia odpowiedzi respondentów grupy nauczyciele akademiccy i grupy studenci (różne kierunki) na temat zagrożeń systemu informacyjnego w uczelni wyższej przez awarie sprzętowe i oprogramowania.

Tabela 3.47. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy studenci (różne kierunki) na temat zagrożeń systemu informacyjnego w uczelni wyższej przez awarie sprzętowe i oprogramowania

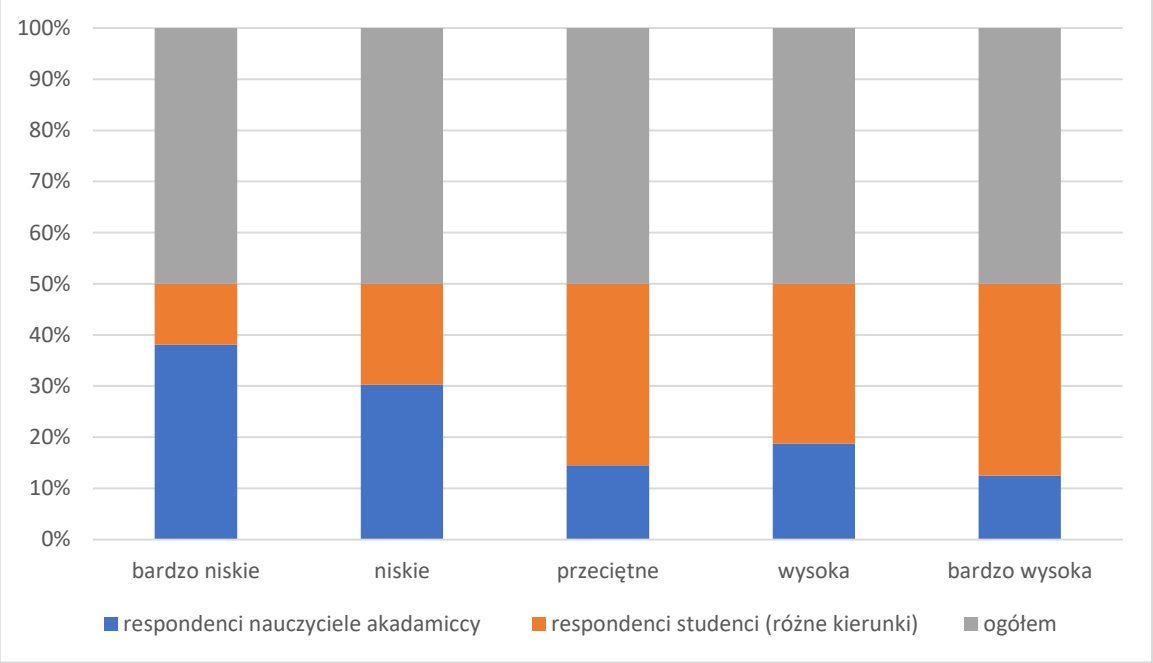
Odpowiedzi badanych osób awarie sprzętowe i oprogramowania						
Osoby poddane badaniu	**Respondenci nauczyciele akademiccy**		**Respondenci studenci (różne kierunki)**		**OGÓŁEM**	
Ocena	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***
bardzo niska	189	37,8%	59	11,8%	248	24,8%
niska	172	34,4%	112	22,4%	284	28,4%
przeciętna	122	24,4%	298	59,6%	420	42%
wysoka	15	3%	25	5%	40	4%
bardzo wysoka	2	0,4%	6	1,2%	8	0,8%
	500	**100%**	**500**	**100%**	**1000**	**100%**

Źródło: opracowanie własne na podstawie badań własnych

W badaniu wzięło udział 500 osób zatrudnionych na stanowisku, nauczycieli akademickich oraz 500 osób studiujących w uczelni wyższej. Z przeprowadzonej analizy wynika, że nauczyciele akademiccy jak i studenci (różne kierunki) ocenili stopień zagrożenia systemu uczelni wyższej przez awarie sprzętowe i oprogramowania, jako bardzo niski i przeciętny. Wskazuje na to 189 respondentów, co w udziale procentowym wynosi 37,8% dla nauczycieli akademickich i 298 respondentów, co w udziale procentowym dla studentów (różne roczniki) wynosi 59,6%.

Analizując udzielone odpowiedzi w opinii 2 respondentów, co w udziale procentowym wynosi 0,4% dla nauczycieli akademickich i 6 respondentów, co w udziale procentowym daje 1,2% dla studentów studiujących w uczelni wyższej świadczy, że pojawienie się awarii sprzętowych i oprogramowania stanowi bardzo duże zagrożenie dla systemu informacyjnego uczelni wyższej. Wykres 3.93. przedstawia odpowiedzi respondentów grupy nauczyciele akademiccy i grupy studenci (różne kierunki) na temat stopnia zagrożenia systemu uczelni wyższej przez awarie sprzętowe i oprogramowania.

Wykres 3.93. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy studenci (różne kierunki) na temat stopnia zagrożenia systemu uczelni wyższej przez awarie sprzętowe i oprogramowania



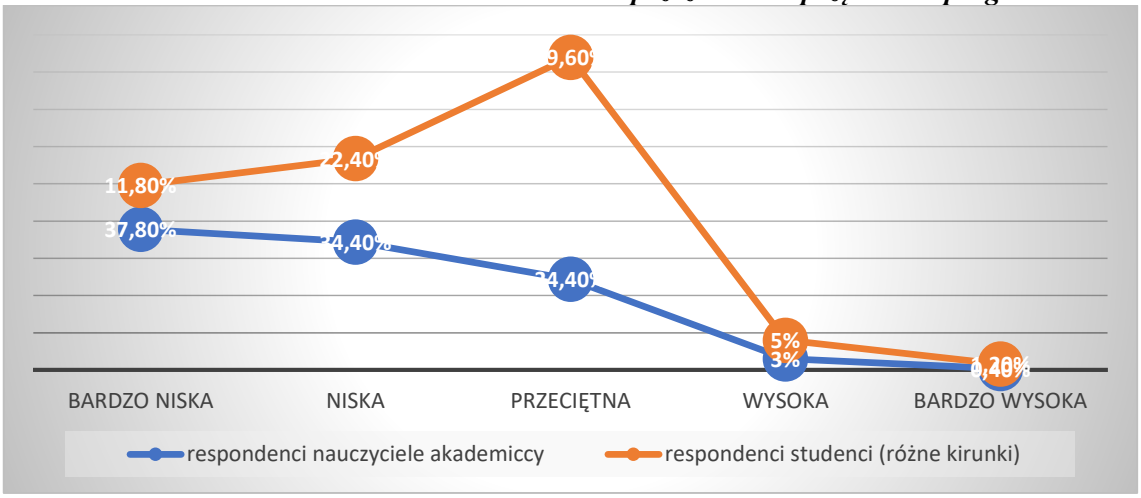
Źródło: opracowanie własne na podstawie badań własnych

O stopniu zależności świadczy współczynnik korelacji liniowej Pearsona na poziomie 0,42 i współczynnik determinacji liniowej, który wskazuje procent wyjaśnionej liniowo zmienności równy 17,64%. Wykres 3.94. pokazuje zależność między respondentami grupy nauczyciele akademiccy i grupy studenci (różne kierunki) pod względem stopnia zagrożenia systemu uczelni wyższej przez awarie sprzętowe i oprogramowania.

$$r_{xy} = \frac{\frac{1}{n}\sum_{i=1}^{n}(x_i-\bar{x})(y_i-\bar{y})}{S_x S_y}=0{,}42$$

$$\mathrm{WD}=r_{xy}^{2} * 100\% = 17{,}64\%$$

Wykres 3.94. Zależność między respondentami grupy nauczyciele akademiccy i grupy studenci (różne kierunki) pod względem stopnia zagrożenia systemu uczelni wyższej przez awarie sprzętowe i oprogramowania



Źródło: opracowanie własne na podstawie badań własnych

W związku z faktem, że wartość liczbowa w ocenie relacji jest dodatnia oznacza to, iż wraz ze wzrostem wartości jednej zmiennej rosną wartości także drugiej. Tabela 3.48. przedstawia odpowiedzi respondentów grupy kadra administracyjna i grupy studenci (różne kierunki) na temat zagrożeń systemu informacyjnego w uczelni wyższej przez awarie sprzętowe i oprogramowania.

Tabela 3.48. Odpowiedzi respondentów grupy kadra administracyjna i grupy studenci (różne kierunki) na temat zagrożeń systemu informacyjnego w uczelni wyższej przez awarie sprzętowe i oprogramowania

Odpowiedzi badanych osób awarie sprzętowe i oprogramowania						
Osoby poddane badaniu	**Respondenci kadra administracyjna**		**Respondenci studenci (różne kierunki)**		**OGÓŁEM**	
Ocena	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***
bardzo niska	139	27,8%	59	11,8%	198	19,8%
niska	169	33,8%	112	22,4%	281	28,1%
przeciętna	182	36,4%	298	59,6%	480	48%
wysoka	9	1,8%	25	5%	34	34%
bardzo wysoka	1	0,2%	6	1,2%	7	0,7%
	500	**100%**	**500**	**100%**	**1000**	**100%**

Źródło: opracowanie własne na podstawie badań własnych

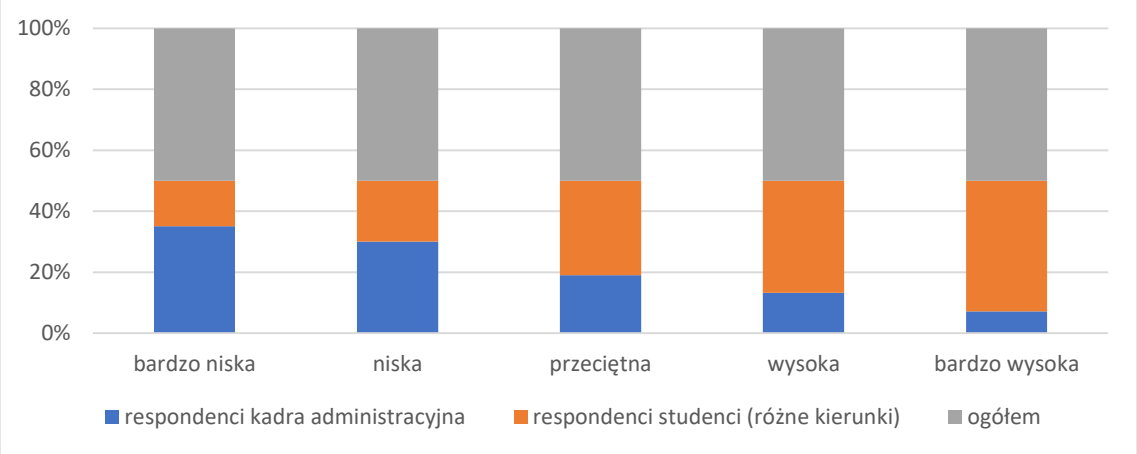
W badaniu wzięło udział 500 osób zatrudnionych na stanowisku, kadra administracyjna oraz 500 osób studiujących w uczelni wyższej. Z przeprowadzonej analizy wynika, że kadra administracyjna jak i studenci (różne kierunki) ocenili stopień zagrożenia

systemu uczelni wyższej przez awarie sprzętowe i oprogramowania, jako przeciętna. Wskazuje na to 182 respondentów, co w udziale procentowym wynosi 36,4% dla kadry administracyjnej i 298 respondentów, co w udziale procentowym dla studentów (różne roczniki) wynosi 59,6%.

Analizując udzielone odpowiedzi w opinii 1 respondenta, co w udziale procentowym wynosi 0,2% dla kadry administracyjnej i 6 respondentów, co w udziale procentowym daje 1,2% dla studentów studiujących w uczelni wyższej świadczy, że pojawienie się awarii sprzętowych i oprogramowania stanowi bardzo duże zagrożenie dla systemu informacyjnego uczelni wyższej.

Wykres 3.95. przedstawia odpowiedzi respondentów grupy kadra administracyjna i grupy studenci (różne kierunki) na temat stopnia zagrożenia systemu uczelni wyższej przez awarie sprzętowe i oprogramowania.

Wykres 3.95. Odpowiedzi respondentów grupy kadra administracyjna i grupy studenci (różne kierunki) na temat stopnia zagrożenia systemu uczelni wyższej przez awarie sprzętowe i oprogramowania



Źródło: opracowanie własne na podstawie badań własnych

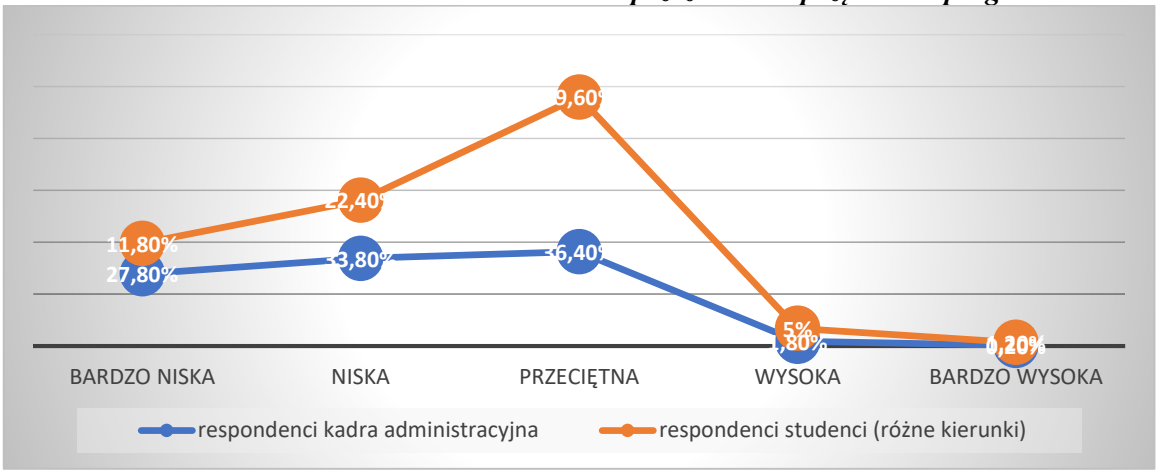
O stopniu zależności świadczy współczynnik korelacji liniowej Pearsona na poziomie 0,76 i współczynnik determinacji liniowej, który wskazuje procent wyjaśnionej liniowo zmienności równy 57,76%.

Wykres 3.96. pokazuje zależność między respondentami grupy kadra administracyjna i grupy studenci (różne kierunki) pod względem stopnia zagrożenia systemu uczelni wyższej przez awarie sprzętowe i oprogramowania.

$$r_{xy} = \frac{\frac{1}{n}\sum_{i=1}^{n}(x_i-\bar{x})(y_i-\bar{y})}{S_x S_y}=0{,}76$$

$$\mathrm{WD}=r_{xy}^{2} * 100\% = 57{,}76\%$$

Wykres 3.96. Zależność między respondentami grupy kadra administracyjna i grupy studenci (różne kierunki) pod względem stopnia zagrożenia systemu uczelni wyższej przez awarie sprzętowe i oprogramowania



Źródło: opracowanie własne na podstawie badań własnych

W związku z faktem, że wartość liczbowa w ocenie relacji jest dodatnia oznacza to, iż wraz ze wzrostem wartości jednej zmiennej rosną wartości także drugiej.

13. Jak Państwo oceniają zagrożenia systemu informacyjnego w uczelni wyższej? q) Pozostawienie danych wrażliwych na biurkach, półkach w miejscach do tego nie-przeznaczonych.

Rozkład odpowiedzi respondentów grupy nauczyciele akademiccy i kadra administracyjna dotyczący oceny użytkowników stopnia zagrożenia systemu uczelni wyższej przez pozostawienie danych wrażliwych na biurkach, półkach w miejscach o tego nie-przeznaczonych prezentuje tabela 3.49.

Tabela 3.49. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy kadra administracyjna na temat zagrożeń systemu informacyjnego w uczelni wyższej przez pozostawienie danych wrażliwych na biurkach, półkach w miejscach do tego nieprzeznaczonych

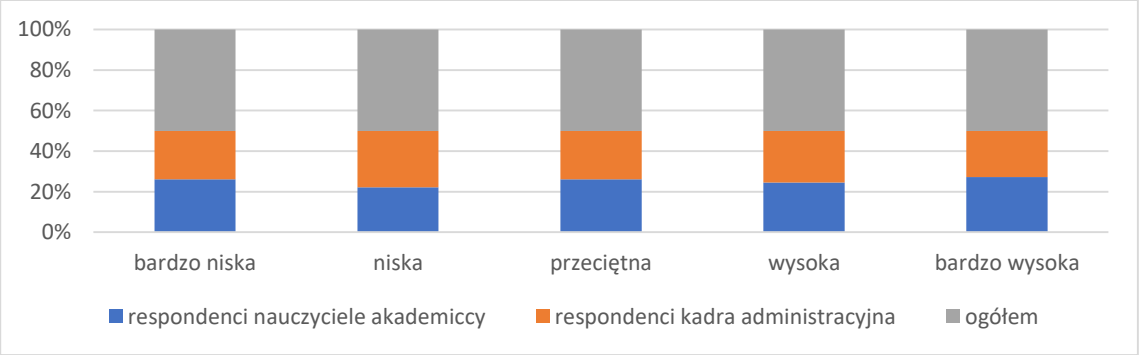
Odpowiedzi badanych osób pozostawienie danych wrażliwych na biurkach, półkach w miejscach do tego nieprzeznaczonych						
Osoby poddane badaniu	**Respondenci nauczyciele akademiccy**		**Respondenci kadra administracyjna**		**OGÓŁEM**	
Ocena	*liczba wskazań*	*udział procentowy*	*liczba wskazań*	*udział procentowy*	*liczba wskazań*	*udział procentowy*
bardzo niska	69	13,8%	63	12,6%	132	13,2%
niska	116	23,2%	146	29,2%	262	26,2%
przeciętna	269	53,8%	246	49,2%	515	51,5%
wysoka	28	5,6%	29	5,8%	57	5,7%
bardzo wysoka	19	3,8%	16	3,2%	35	3,5%
	500	**100%**	**500**	**100%**	**1000**	**100%**

Źródło: opracowanie własne na podstawie badań własnych

W badaniu wzięło udział 500 osób zatrudnionych na stanowisku, nauczycieli akademickich oraz 500 osób zatrudnionych na stanowisku kadra administracyjna. Z przeprowadzonej analizy wynika, że nauczyciele akademiccy jak i kadra administracyjna ocenili stopień zagrożenia systemu uczelni wyższej przez pozostawienie danych wrażliwych na biurkach, półkach w miejscach do tego nieprzeznaczonych, jako przeciętny. Wskazuje na to 269 respondentów, co w udziale procentowym wynosi 53,8% dla nauczycieli akademickich i 246 respondentów, co w udziale procentowym dla kadry administracyjnej wynosi 49,2%.

Analizując udzielone odpowiedzi w opinii 19 respondentów, co w udziale procentowym wynosi 3,8% dla nauczycieli akademickich i 16 respondentów, co w udziale procentowym daje 3,2% dla kadry administracyjnej świadczy, że pojawienie się pozostawionych danych wrażliwych na biurkach, półkach w miejscach do tego nieprzeznaczonych stanowi bardzo duże zagrożenie dla systemu informacyjnego uczelni wyższej. Wykres 3.97. przedstawia odpowiedzi respondentów grupy nauczyciele akademiccy i grupy kadra administracyjna na temat stopnia zagrożenia systemu uczelni wyższej przez pozostawienie danych wrażliwych na biurkach, półkach w miejscach do tego nieprzeznaczonych.

Wykres 3.97. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy kadra administracyjna na temat stopnia zagrożenia systemu uczelni wyższej przez pozostawienie danych wrażliwych na biurkach, półkach w miejscach do tego nieprzeznaczonych



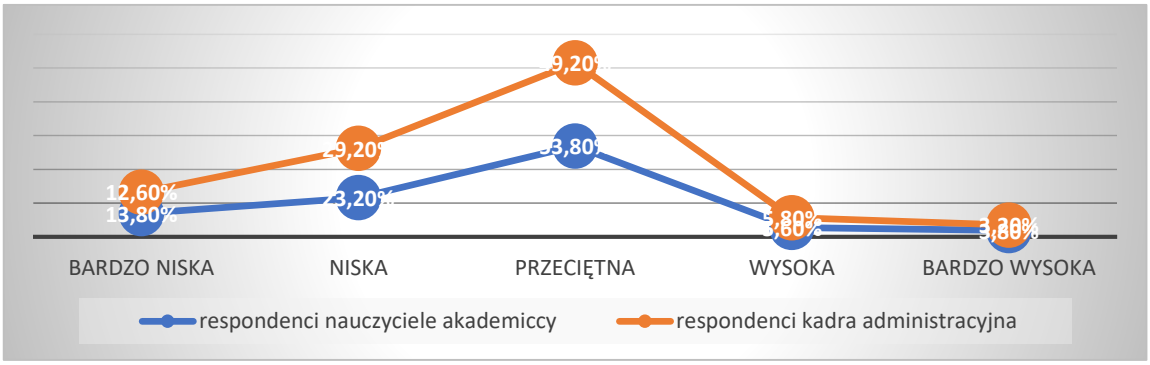
Źródło: opracowanie własne na podstawie badań własnych

O stopniu zależności świadczy współczynnik korelacji liniowej Pearsona na poziomie 0,98 i współczynnik determinacji liniowej, który wskazuje procent wyjaśnionej liniowo zmienności równy 96,04%. Wykres 3.98. pokazuje zależność między respondentami grupy nauczyciele akademiccy i grupy kadra administracyjna pod względem stopnia zagrożenia systemu uczelni wyższej przez pozostawienie danych wrażliwych na biurkach, półkach w miejscach do tego nieprzeznaczonych.

$$r_{xy} = \frac{\frac{1}{n}\sum_{i=1}^{n}(x_i-\bar{x})(y_i-\bar{y})}{s_x s_y}=0{,}98$$

$$WD=r\frac{2}{xy} * 100\% = 96{,}04\%$$

Wykres 3.98. Zależność między respondentami grupy nauczyciele akademiccy i grupy kadra administracyjna pod względem stopnia zagrożenia systemu uczelni wyższej



przez pozostawienie danych wrażliwych na biurkach, półkach w miejscach do tego nieprzeznaczonych

Źródło: opracowanie własne na podstawie badań własnych

W związku z faktem, że wartość liczbowa w ocenie relacji jest dodatnia oznacza to, iż wraz ze wzrostem wartości jednej zmiennej rosną wartości także drugiej. Tabela 3.50. przedstawia odpowiedzi respondentów grupy nauczyciele akademiccy i grupy studenci (różne kierunki) na temat zagrożeń systemu informacyjnego w uczelni wyższej przez pozostawienie danych wrażliwych na biurkach, półkach w miejscach do tego nieprzeznaczonych.

Tabela 3.50. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy studenci (różne kierunki) na temat zagrożeń systemu informacyjnego w uczelni wyższej przez pozostawienie danych wrażliwych na biurkach, półkach w miejscach do tego nieprzeznaczonych

Odpowiedzi badanych osób pozostawienie danych wrażliwych na biurkach, półkach w miejscach do tego nieprzeznaczonych						
Osoby poddane badaniu	**Respondenci nauczyciele akademiccy**		**Respondenci studenci (różne kierunki)**		**OGÓŁEM**	
Ocena	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***
bardzo niska	69	13,8%	169	33,8%	238	23,8%
niska	116	23,2%	158	31,6%	274	27,4%
przeciętna	269	53,8%	162	32,4%	421	42,1%
wysoka	28	5,6%	8	1,6%	36	3,6%
bardzo wysoka	19	3,8%	3	0,6%	22	2,2%
	500	**100%**	**500**	**100%**	**1000**	**100%**

Źródło: opracowanie własne na podstawie badań własnych

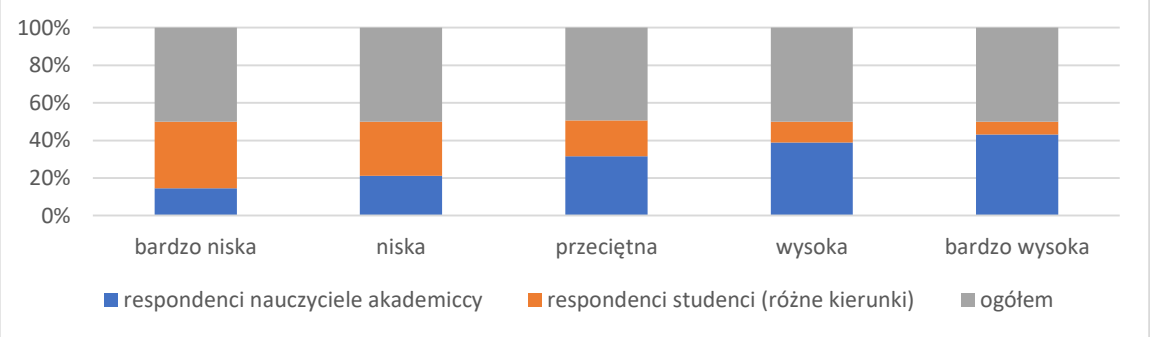
W badaniu wzięło udział 500 osób zatrudnionych na stanowisku, nauczycieli akademickich oraz 500 osób studiujących w uczelni wyższej. Z przeprowadzonej analizy wynika, że nauczyciele akademiccy jak i studenci (różne kierunki) ocenili stopień zagro-

żenia systemu uczelni wyższej przez pozostawienie danych wrażliwych na biurkach, półkach w miejscach do tego nieprzeznaczonych, jako przeciętny i bardzo niski. Wskazuje na to 269 respondentów, co w udziale procentowym wynosi 53,8% dla nauczycieli akademickich i 169 respondentów, co w udziale procentowym dla studentów (różne roczniki) wynosi 33,8%.

Analizując udzielone odpowiedzi w opinii 19 respondentów, co w udziale procentowym wynosi 3,8% dla nauczycieli akademickich i 3 respondentów, co w udziale procentowym daje 0,6% dla studentów studiujących w uczelni wyższej świadczy, że pojawienie się pozostawionych danych wrażliwych na biurkach, półkach w miejscach do tego nieprzeznaczonych stanowi bardzo duże zagrożenie dla systemu informacyjnego uczelni wyższej.

Wykres 3.99. przedstawia odpowiedzi respondentów grupy nauczyciele akademiccy i grupy studentów (różne kierunki) na temat stopnia zagrożenia systemu uczelni wyższej przez pozostawienie danych wrażliwych na biurkach, półkach w miejscach do tego nieprzeznaczonych.

Wykres 3.99. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy studenci (różne kierunki) na temat stopnia zagrożenia systemu uczelni wyższej przez pozostawienie danych wrażliwych na biurkach, półkach w miejscach do tego nieprzeznaczonych



Źródło: opracowanie własne na podstawie badań własnych

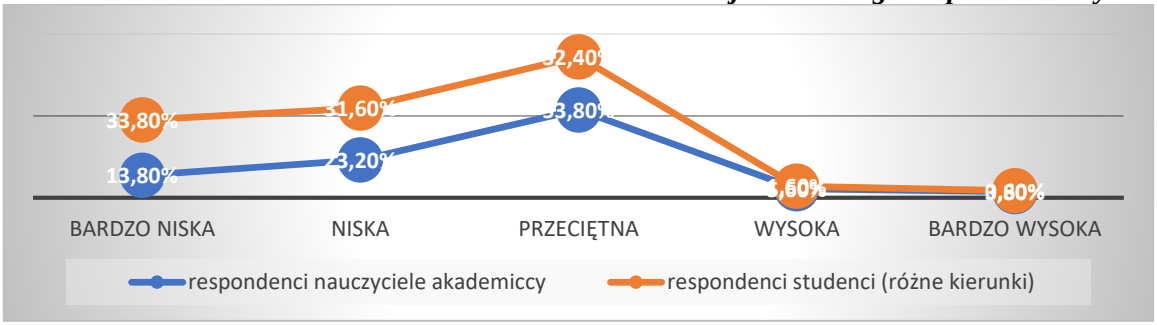
O stopniu zależności świadczy współczynnik korelacji liniowej Pearsona na poziomie 0,67 i współczynnik determinacji liniowej, który wskazuje procent wyjaśnionej liniowo zmienności równy 44,89%.

Wykres 3.100. pokazuje zależność między respondentami grupy nauczyciele akademiccy i grupy studenci pod względem stopnia zagrożenia systemu uczelni wyższej przez pozostawienie danych wrażliwych na biurkach, półkach w miejscach do tego nieprzeznaczonych.

$$r_{xy} = \frac{\frac{1}{n}\sum_{i=1}^{n}(x_i-\bar{x})(y_i-\bar{y})}{S_x S_y}=0{,}67$$

$$WD=r\frac{2}{xy} * 100\% = 44{,}89\%$$

Wykres 148 Wykres 3.100. Zależność między respondentami grupy nauczyciele akademiccy i grupy studenci (różne kierunki) pod względem stopnia zagrożenia systemu uczelni wyższej przez pozostawienie danych wrażliwych na biurkach, półkach w miejscach do tego nieprzeznaczonych



Źródło: opracowanie własne na podstawie badań własnych

W związku z faktem, że wartość liczbowa w ocenie relacji jest dodatnia oznacza to, iż wraz ze wzrostem wartości jednej zmiennej rosną wartości także drugiej. Tabela 3.51. przedstawia odpowiedzi respondentów grupy kadra administracyjna i grupy studenci (różne kierunki) na temat zagrożeń systemu informacyjnego w uczelni wyższej przez pozostawienie danych wrażliwych na biurkach, półkach w miejscach do tego nieprzeznaczonych.

Tabela 3.51. Odpowiedzi respondentów grupy kadra administracyjna i grupy studenci (różne kierunki) na temat zagrożeń systemu informacyjnego w uczelni wyższej przez pozostawienie danych wrażliwych na biurkach, półkach w miejscach do tego nieprzeznaczonych

Odpowiedzi badanych osób pozostawienie danych wrażliwych na biurkach, półkach w miejscach do tego nieprzeznaczonych						
Osoby poddane badaniu	**Respondenci kadra administracyjna**		**Respondenci studenci (różne kierunki)**		**OGÓŁEM**	
Ocena	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***
bardzo niska	63	12,6%	169	33,8%	232	23,2%
niska	146	29,2%	158	31,6%	304	30,4%
przeciętna	246	49,2%	162	32,4%	408	40,8%
wysoka	29	5,8%	8	1,6%	37	3,7%
bardzo wysoka	16	3,2%	3	0,6%	19	1,9%
	500	**100%**	**500**	**100%**	**1000**	**100%**

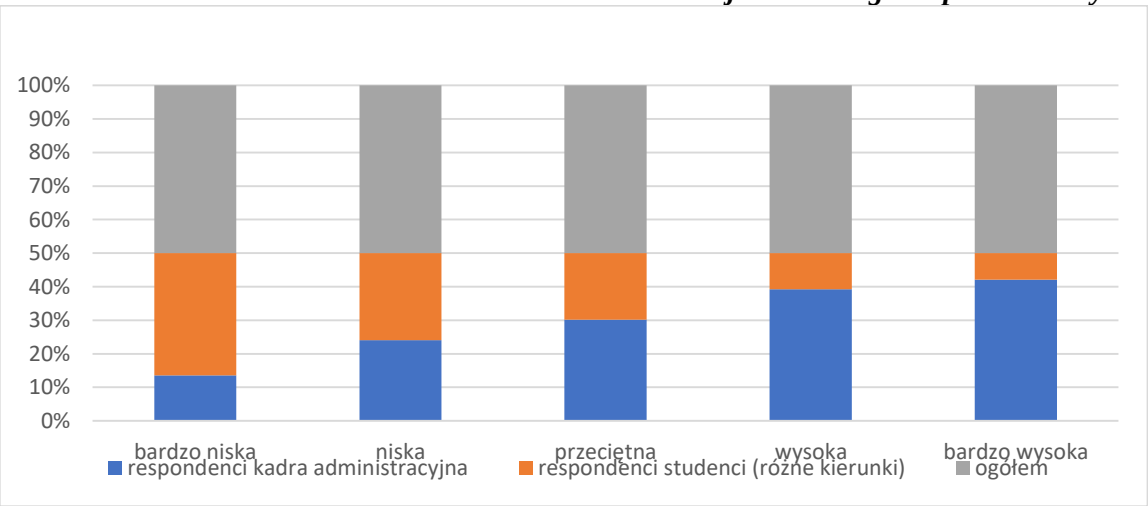
Źródło: opracowanie własne na podstawie badań własnych

W badaniu wzięło udział 500 osób zatrudnionych na stanowisku, kadra administracyjna oraz 500 osób studiujących w uczelni wyższej. Z przeprowadzonej analizy wynika, że kadra administracyjna jak i studenci (różne kierunki) ocenili stopień zagrożenia systemu uczelni wyższej przez pozostawienie danych wrażliwych na biurkach, półkach w miejscach do tego nieprzeznaczonych, jako przeciętny i bardzo niski. Wskazuje na to

246 respondentów, co w udziale procentowym wynosi 49,2% dla kadry administracyjnej i 169 respondentów, co w udziale procentowym dla studentów (różne roczniki) wynosi 33,8%.

Analizując udzielone odpowiedzi w opinii 16 respondentów, co w udziale procentowym wynosi 3,2% dla kadry administracyjnej i 3 respondentów, co w udziale procentowym daje 0,6% dla studentów studiujących w uczelni wyższej świadczy, że pojawienie się pozostawionych danych wrażliwych na biurkach, półkach w miejscach do tego nieprzeznaczonych stanowi bardzo duże zagrożenie dla systemu informacyjnego uczelni wyższej. Wykres 3.101. przedstawia odpowiedzi respondentów grupy kadry administracyjnej i grupy studentów (różne kierunki) na temat stopnia zagrożenia systemu uczelni wyższej przez pozostawienie danych wrażliwych na biurkach, półkach w miejscach do tego nieprzeznaczonych.

Wykres 3.101. Odpowiedzi respondentów grupy kadra administracyjna i grupy studenci (różne kierunki) na temat stopnia zagrożenia systemu uczelni wyższej przez pozostawienie danych wrażliwych na biurkach, półkach w miejscach do tego nieprzeznaczonych



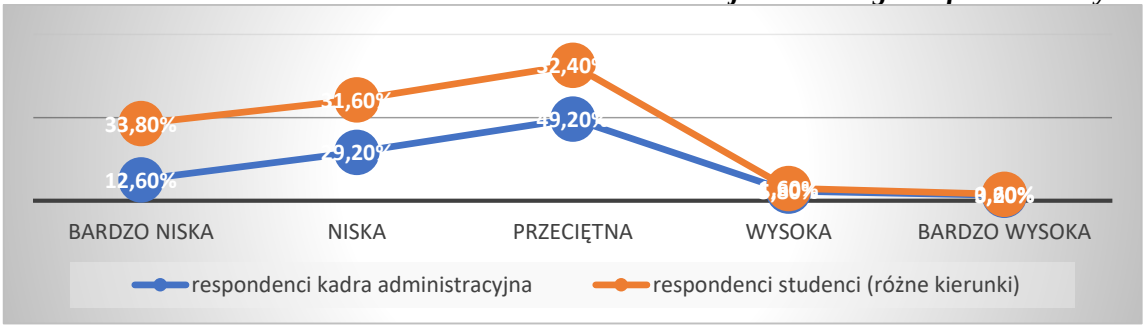
Źródło: opracowanie własne na podstawie badań własnych

O stopniu zależności świadczy współczynnik korelacji liniowej Pearsona na poziomie 0,72 i współczynnik determinacji liniowej, który wskazuje procent wyjaśnionej liniowo zmienności równy 51,84%. Wykres 3.102. pokazuje zależność między respondentami grupy kadra administracyjna i grupy studenci pod względem stopnia zagrożenia systemu uczelni wyższej przez pozostawienie danych wrażliwych na biurkach, półkach w miejscach do tego nieprzeznaczonych.

$$r_{xy} = \frac{\frac{1}{n}\sum_{i=1}^{n}(x_i-\bar{x})(y_i-\bar{y})}{S_x S_y}=0{,}72$$

$$\mathrm{WD}=r_{xy}^{2} * 100\% = 51{,}84\%$$

Wykres 3.102. Zależność między respondentami grupy kadra administracyjna i grupy studenci (różne kierunki) pod względem stopnia zagrożenia systemu uczelni wyższej przez pozostawienie danych wrażliwych na biurkach, półkach w miejscach do tego nieprzeznaczonych



Źródło: opracowanie własne na podstawie badań własnych

W związku z faktem, że wartość liczbowa w ocenie relacji jest dodatnia oznacza to, iż wraz ze wzrostem wartości jednej zmiennej rosną wartości także drugiej.

14. Kto według Państwa jest najczęstszym odbiorcą Państwa informacji w systemie?

Rozkład odpowiedzi przez respondentów grupy nauczyciele akademiccy i kadra administracyjna odnośnie odbiorców informacji w systemie uczelni wyższej prezentuje tabela 3.52.

Tabela 3.52. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy kadra administracyjna na temat odbiorców informacji w uczelni wyższej

Odpowiedzi badanych osób odbiór informacji w systemie						
Osoby poddane badaniu	**Respondenci nauczyciele akademiccy**		**Respondenci kadra administracyjna**		**OGÓŁEM**	
Ocena	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***
Rektor/Prorektorzy/Władze Uczelni	15	3%	32	6,4%	47	4,7%
Dyrektorzy Instytutów	25	5%	49	9,8%	74	7,4%
Centrum Obsługi studenta	6	1,2%	65	13%	71	7,1%
Kancelaria uczelni	158	31,6%	158	31,6%	316	31,6%
Sekretariat (jednostki administracyjne)	296	59,2%	196	39,2%	492	49,2%
	500	**100%**	**500**	**100%**	**1000**	**100%**

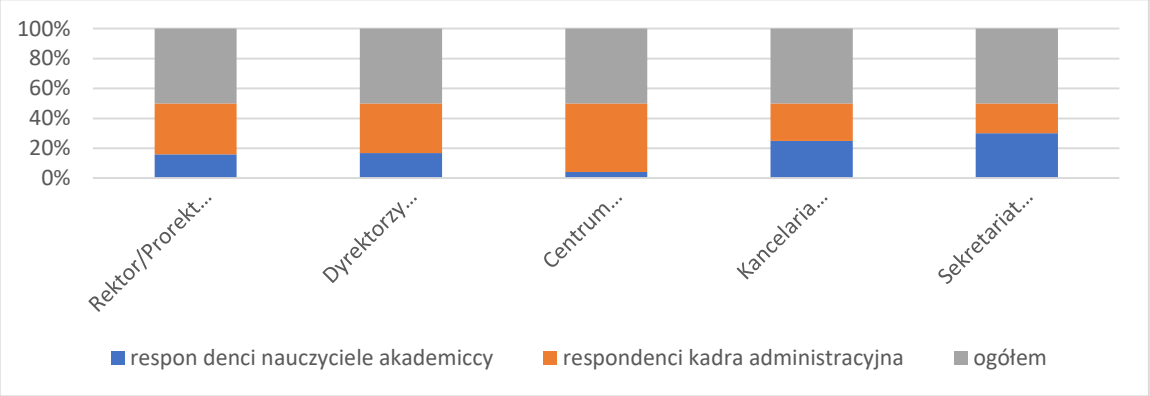
Źródło: opracowanie własne na podstawie badań własnych

W badaniu wzięło udział 500 osób zatrudnionych na stanowisku, nauczycieli akademickich oraz 500 osób zatrudnionych na stanowisku kadra administracyjna. Z przeprowadzonej analizy wynika, że najczęstszym odbiorcą dokumentów jest sekretariat, zarówno dla grupy nauczyciele akademiccy jak i kadra administracyjna. Wskazuje na to 296 respondentów, co w udziale procentowym wynosi 59,2% dla nauczycieli akademickich i 196 respondentów, co w udziale procentowym dla kadry administracyjnej wynosi 39,2%.

Analizując udzielone odpowiedzi w opinii 158 respondentów, co w udziale procentowym wynosi 31,6% dla nauczycieli akademickich i 158 respondentów, co w udziale procentowym daje 31,6% dla kadry administracyjnej świadczy, że drugim najczęstszym odbiorcą jest kancelaria uczelni zarówno dla grupy nauczyciele akademiccy i kadra administracyjna.

Wykres 3.103. przedstawia odpowiedzi respondentów grupy nauczyciele akademiccy i grupy kadra administracyjna na temat odbiorców informacji w uczelni wyższej.

Wykres 3.103. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy kadra administracyjna na temat najczęstszego odbiorcy informacji w systemie



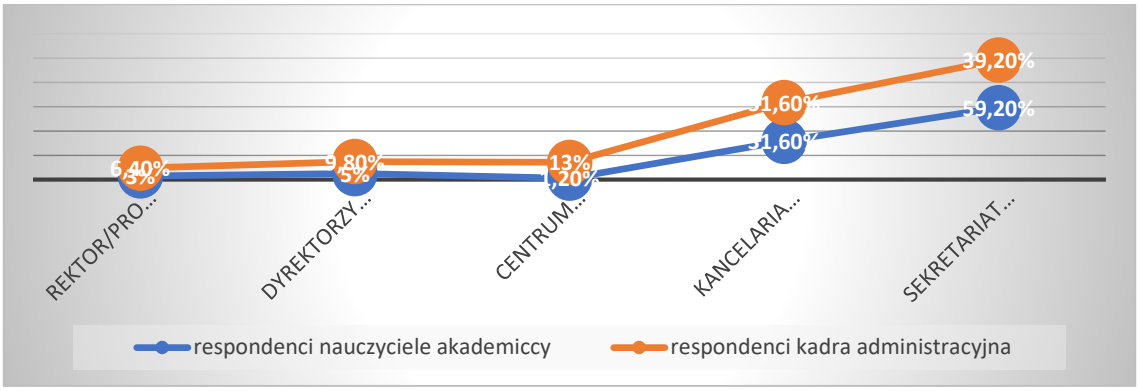
Źródło: opracowanie własne na podstawie badań własnych

O stopniu zależności świadczy współczynnik korelacji liniowej Pearsona na poziomie 0,96 i współczynnik determinacji liniowej, który wskazuje procent wyjaśnionej liniowo zmienności równy 92,16%. Wykres 3.104. pokazuje zależność między respondentami grupy nauczyciele akademiccy i grupy kadra administracyjna na temat odbiorców informacji w uczelni wyższej.

$$r_{xy} = \frac{\frac{1}{n}\sum_{i=1}^{n}(x_i-\bar{x})(y_i-\bar{y})}{S_x S_y}=0{,}96$$

$$\mathrm{WD}=r_{xy}^{2} * 100\% = 92{,}16\%$$

Wykres 3.104. Zależność między respondentami grupy nauczyciele akademiccy i grupy kadra administracyjna temat odbiorców informacji w uczelni wyższej



Źródło: opracowanie własne na podstawie badań własnych

W związku z faktem, że wartość liczbowa w ocenie relacji jest dodatnia oznacza to, iż wraz ze wzrostem wartości jednej zmiennej rosną wartości także drugiej. Tabela 3.53. przedstawia odpowiedzi respondentów grupy nauczyciele akademiccy i grupy studenci (różne kierunki) temat odbiorców informacji w uczelni wyższej.

Tabela 3.53. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy studenci (różne kierunki) na temat odbiorców informacji w uczelni wyższej

Odpowiedzi badanych osób odbiór informacji w systemie						
Osoby poddane badaniu	**Respondenci nauczyciele akademiccy**		**Respondenci studenci (różne kierunki)**		**OGÓŁEM**	
Ocena	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***
Rektor/Prorektorzy/Władze Uczelni	15	3%	2	0,4%	17	1,7%
Dyrektorzy Instytutów	25	5%	6	1,2%	31	3,1%
Centrum Obsługi studenta	6	1,2%	172	34,4%	178	17,8%
Kancelaria uczelni	158	31,6%	152	30,4%	310	31%
Sekretariat (jednostki administracyjne)	296	59,2%	168	33,6%	464	46,4%
	500	**100%**	**500**	**100%**	**1000**	**100%**

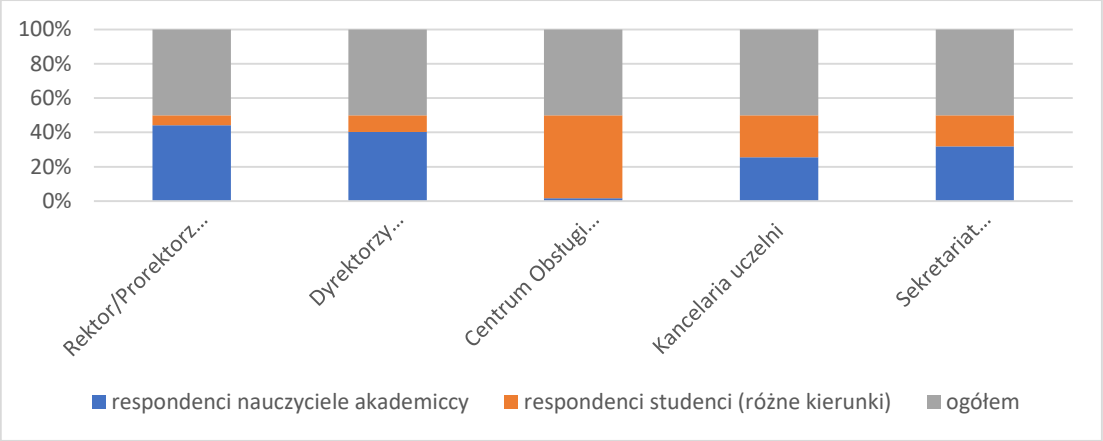
Źródło: opracowanie własne na podstawie badań własnych

W badaniu wzięło udział 500 osób zatrudnionych na stanowisku, nauczycieli akademickich oraz 500 osób studiujących w uczelni wyższej. Z przeprowadzonej analizy wynika, że najczęstszym odbiorcą dokumentów jest sekretariat, dla grupy kadra administracyjna i centrum obsługi studenta dla studentów. Wskazuje na to 296 respondentów,

co w udziale procentowym wynosi 59,2% dla nauczycieli akademickich i 172 respondentów, co w udziale procentowym dla grupy studentów wynosi 34,4%.

Analizując udzielone odpowiedzi w opinii 15 respondentów, co w udziale procentowym wynosi 3% dla nauczycieli akademickich i 2 respondentów, co w udziale procentowym daje 0,4% dla studentów (różne kierunki) świadczy, że najrzadszym odbiorcą informacji w systemie są władze uczelni. Wykres 3.105. przedstawia odpowiedzi respondentów grupy nauczyciele akademiccy i grupy studenci (różne kierunki) na temat odbiorców informacji w uczelni wyższej.

Wykres 3.105. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy studenci (różne kierunki) na temat najczęstszego odbiorcy informacji w systemie



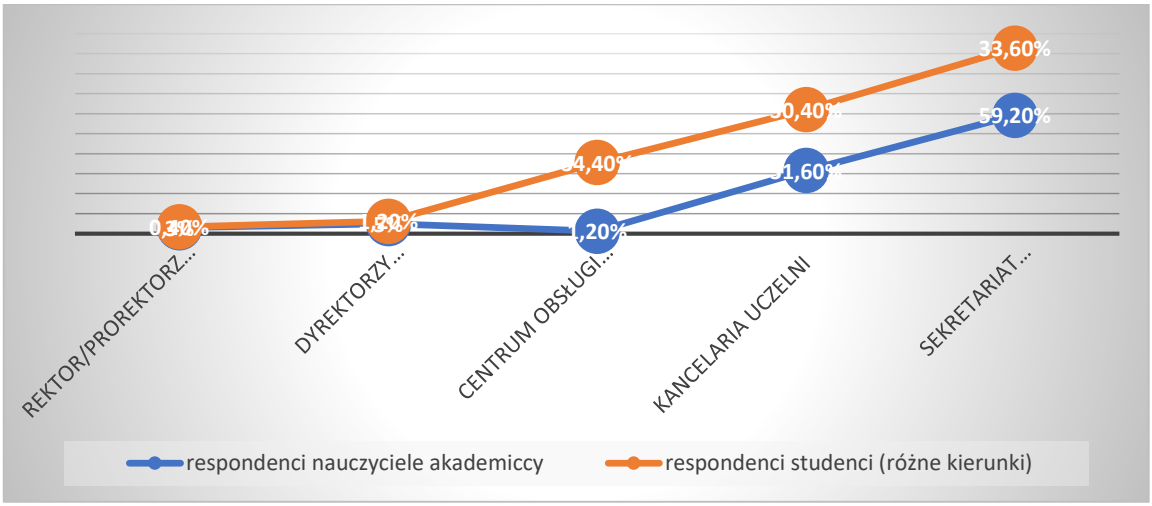
Źródło: opracowanie własne na podstawie badań własnych

O stopniu zależności świadczy współczynnik korelacji liniowej Pearsona na poziomie 0,56 i współczynnik determinacji liniowej, który wskazuje procent wyjaśnionej liniowo zmienności równy 31,36%. Wykres 3.106. pokazuje zależność między respondentami grupy nauczyciele akademiccy i grupy studenci (różne kierunki) na temat odbiorców informacji w uczelni wyższej.

$$r_{xy} = \frac{\frac{1}{n}\sum_{i=1}^{n}(x_i-\bar{x})(y_i-\bar{y})}{S_x S_y}=0{,}56$$

$$\mathrm{WD}=r_{xy}^{2} * 100\% = 31{,}36\%$$

Wykres 3.106. Zależność między respondentami grupy nauczyciele akademiccy i grupy studenci (różne kierunki) na temat odbiorców informacji w uczelni wyższej



Źródło: opracowanie własne na podstawie badań własnych

W związku z faktem, że wartość liczbowa w ocenie relacji jest dodatnia oznacza to, iż wraz ze wzrostem wartości jednej zmiennej rosną wartości także drugiej. Tabela 3.54. przedstawia odpowiedzi respondentów grupy kadra administracyjna i grupy studenci (różne kierunki) temat odbiorców informacji w uczelni wyższej

Tabela 3.54. Odpowiedzi respondentów grupy kadra administracyjna i grupy studenci (różne kierunki) na temat odbiorców informacji w uczelni wyższej

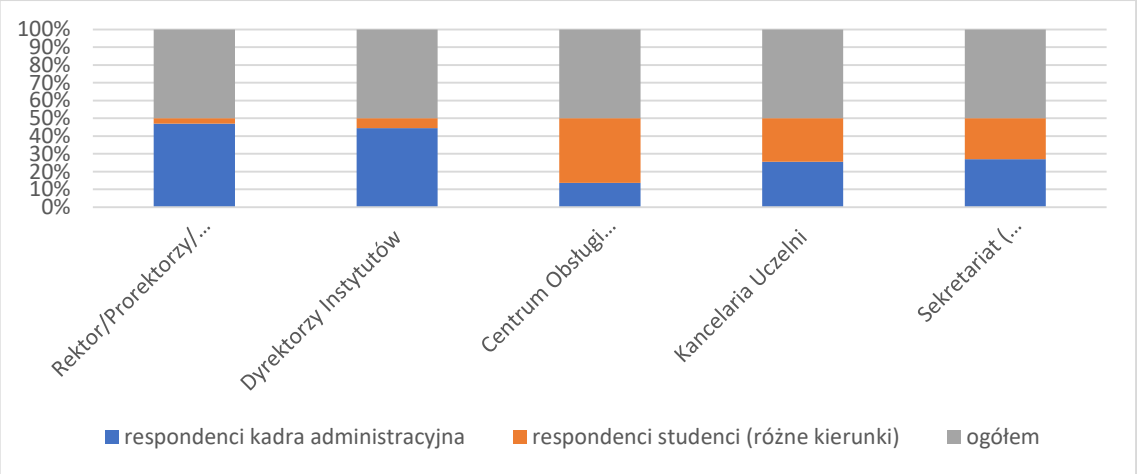
Odpowiedzi badanych osób odbiór informacji w systemie						
Osoby poddane badaniu	**Respondenci kadra administracyjna**		**Respondenci studenci (różne kierunki)**		**OGÓŁEM**	
Ocena	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***
Rektor/Prorektorzy/Władze Uczelni	32	6,4%	2	0,4%	34	3,4%
Dyrektorzy Instytutów	49	9,8%	6	1,2%	55	5,5%
Centrum Obsługi studenta	65	13%	172	34,4%	237	23,7%
Kancelaria Uczelni	158	31,6%	152	30,4%	310	31%
Sekretariat (jednostki administracyjne)	196	39,2%	168	33,6%	364	36,4%
	500	**100%**	**500**	**100%**	**1000**	**100%**

Źródło: opracowanie własne na podstawie badań własnych

W badaniu wzięło udział 500 osób zatrudnionych na stanowisku, kadra administracyjna oraz 500 osób studiujących w uczelni wyższej. Z przeprowadzonej analizy wynika, że dyrektorzy instytutów są na czwartym miejscu, jako odbiorcy informacji w systemie dla kadry administracyjnej i studentów (różne kierunki). Wskazuje na to 49 respondentów, co w udziale procentowym wynosi 9,8% dla kadry administracyjnej i 6 respondentów, co w udziale procentowym dla grupy studentów wynosi 1,2%.

Wykres 3.107. przedstawia odpowiedzi respondentów grupy kadra administracyjna i grupy studenci (różne kierunki) na temat odbiorców informacji w uczelni wyższej.

Wykres 3.107. Odpowiedzi respondentów grupy kadra administracyjna i grupy studenci (różne kierunki) na temat najczęstszego odbiorcy informacji w systemie



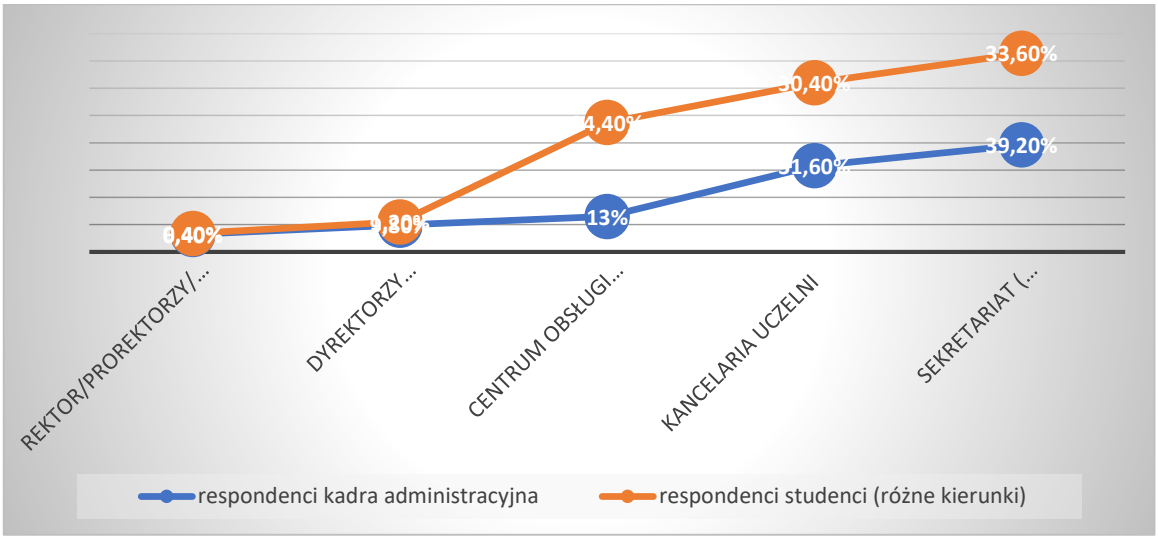
Źródło: opracowanie własne na podstawie badań własnych

O stopniu zależności świadczy współczynnik korelacji liniowej Pearsona na poziomie 0,72 i współczynnik determinacji liniowej, który wskazuje procent wyjaśnionej liniowo zmienności równy 51,84%. Wykres 3.108. pokazuje zależność między respondentami grupy kadra administracyjna i grupy studenci (różne kierunki) na temat odbiorców informacji w uczelni wyższej.

$$r_{xy} = \frac{\frac{1}{n}\sum_{i=1}^{n}(x_i-\bar{x})(y_i-\bar{y})}{s_x s_y}=0{,}72$$

$$\mathrm{WD}=r_{xy}^{2} * 100\% = 51{,}84\%$$

Wykres 3.108. Zależność między respondentami grupy kadra administracyjna i grupy studenci (różne kierunki) na temat odbiorców informacji w uczelni wyższej



Źródło: opracowanie własne na podstawie badań własnych

W związku z faktem, że wartość liczbowa w ocenie relacji jest dodatnia oznacza to, iż wraz ze wzrostem wartości jednej zmiennej rosną wartości także drugiej.

16. Co Państwa zdaniem jest najczęstszym problemem w sprawach działania systemu w uczelni wyższej?

a) Brak dostępu do Internetu

Rozkład odpowiedzi respondentów grupy nauczyciele akademiccy i grupy kadra administracyjna dotyczący oceny przez użytkowników stopnia problemów związanych z brakiem dostępu do Internetu w uczelni wyższej prezentuje tabela 3.55.

Tabela 82 Tabela 3.55. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy kadra administracyjna na temat braku dostępu do Internetu w uczelni wyższej

Odpowiedzi badanych osób brak dostępu do Internetu						
Osoby poddane badaniu	**Respondenci nauczyciele akademiccy**		**Respondenci kadra administracyjna**		**OGÓŁEM**	
Ocena	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***
sporadycznie	103	20,6%	76	15,2%	179	17,9%
niska	156	31,2%	102	20,4%	258	25,8%
przeciętna	118	23,6%	269	53,8%	387	38,7%
wysoka	89	17,8%	36	7,2%	125	12,5%
bardzo wysoka	34	6,8%	17	3,4%	51	5,1%
	500	**100%**	**500**	**100%**	**1000**	**100%**

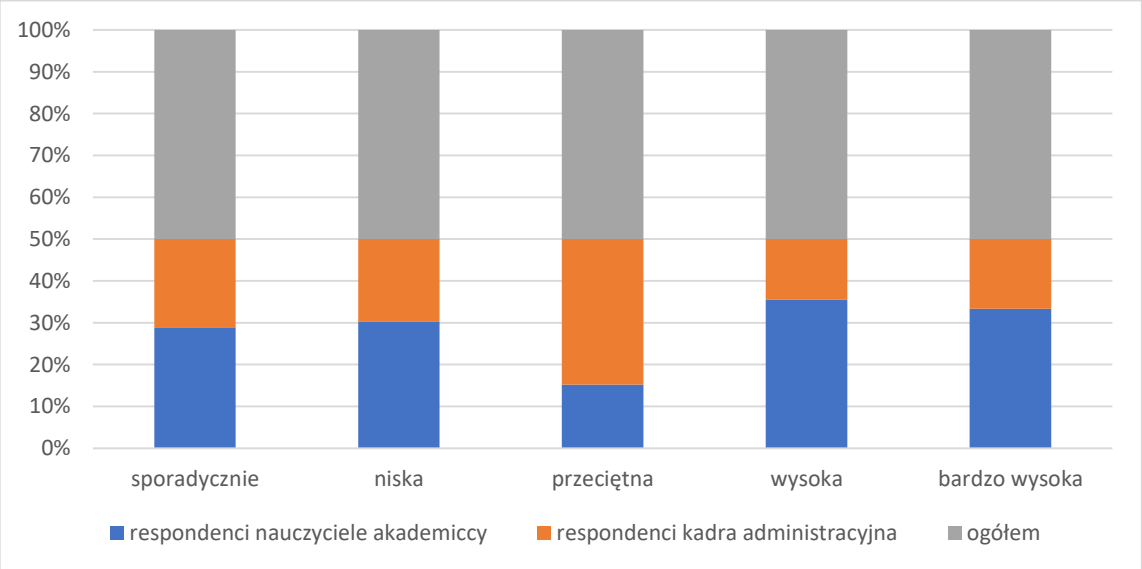
Źródło: opracowanie własne na podstawie badań własnych

W badaniu wzięło udział 500 osób zatrudnionych na stanowisku, nauczycieli akademickich oraz 500 osób zatrudnionych na stanowisku kadry administracyjnej. Z przeprowadzonej analizy wynika, że nauczyciele akademiccy jak i kadra administracyjna ocenili brak dostępu do Internetu w uczelni wyższej w stopniu niskim i przeciętnym. Wskazuje na to 156 respondentów, co w udziale procentowym wynosi 31,2% dla nauczycieli akademickich i 269 respondentów, co w udziale procentowym dla kadry administracyjnej wynosi 53,8%.

Analizując udzielone odpowiedzi w opinii 34 respondentów, co w udziale procentowym wynosi 6,8% dla nauczycieli akademickich i 17 respondentów, co w udziale procentowym daje 3,4% dla kadry administracyjnej świadczy, że pojawienie się braku dostępu do Internetu stanowi bardzo duże zagrożenie dla systemu informacyjnego uczelni wyższej.

Wykres 3.109. przedstawia odpowiedzi respondentów grupy nauczyciele akademiccy i grupy kadra administracyjna na temat braku dostępu do Internetu w uczelni wyższej.

Wykres 3.109. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy kadra administracyjna na temat braku dostępu do Internetu w uczelni wyższej



Źródło: opracowanie własne na podstawie badań własnych

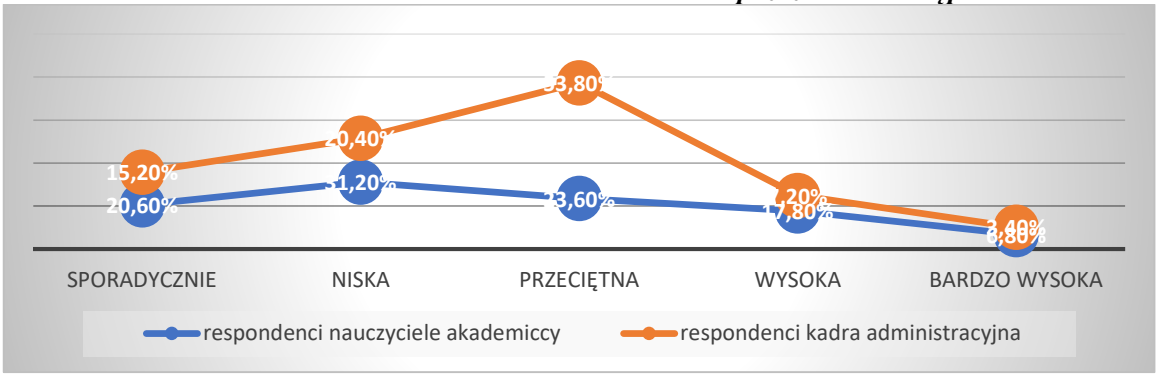
O stopniu zależności świadczy współczynnik korelacji liniowej Pearsona na poziomie 0,52 i współczynnik determinacji liniowej, który wskazuje procent wyjaśnionej liniowo zmienności równy 27,04%.

Wykres 3.110. pokazuje zależność między respondentami grupy nauczyciele akademiccy i grupy kadra administracyjna pod względem stopnia zagrożenia systemu uczelni wyższej przez brak dostępu do Internetu.

$$r_{xy} = \frac{\frac{1}{n}\sum_{i=1}^{n}(x_i-\bar{x})(y_i-\bar{y})}{S_x S_y}=0{,}52$$

$$\text{WD}=r_{xy}^{2} * 100\% = 27{,}04\%$$

Wykres 3.110. Zależność między respondentami grupy nauczyciele akademiccy i grupy kadra administracyjna pod względem stopnia zagrożenia systemu uczelni wyższej przez braku dostępu do Internetu



Źródło: opracowanie własne na podstawie badań własnych

W związku z faktem, że wartość liczbowa w ocenie relacji jest dodatnia oznacza to, iż wraz ze wzrostem wartości jednej zmiennej rosną wartości także drugiej. Tabela 3.56. przedstawia odpowiedzi respondentów grupy nauczyciele akademiccy i grupy studenci (różne kierunki) na temat zagrożeń systemu informacyjnego w uczelni wyższej ze względu na brak dostępu do Internetu w uczelni wyższej.

Tabela 3.56. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy studenci (różne kierunki) na temat braku dostępu do Internetu w uczelni wyższej

Odpowiedzi badanych osób brak dostępu do Internetu						
Osoby poddane badaniu	**Respondenci nauczyciele akademiccy**		**Respondenci studenci (różne kierunki)**		**OGÓŁEM**	
Ocena	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***
sporadycznie	103	20,6%	89	17,8%	192	19,2%
niska	156	31,2%	112	22,4%	268	26,8%
przeciętna	118	23,6%	236	47,2%	354	35,4%
wysoka	89	17,8%	34	6,8%	123	12,3%
bardzo wysoka	34	6,8%	29	5,8%	63	6,3%
	500	**100%**	**500**	**100%**	**1000**	**100%**

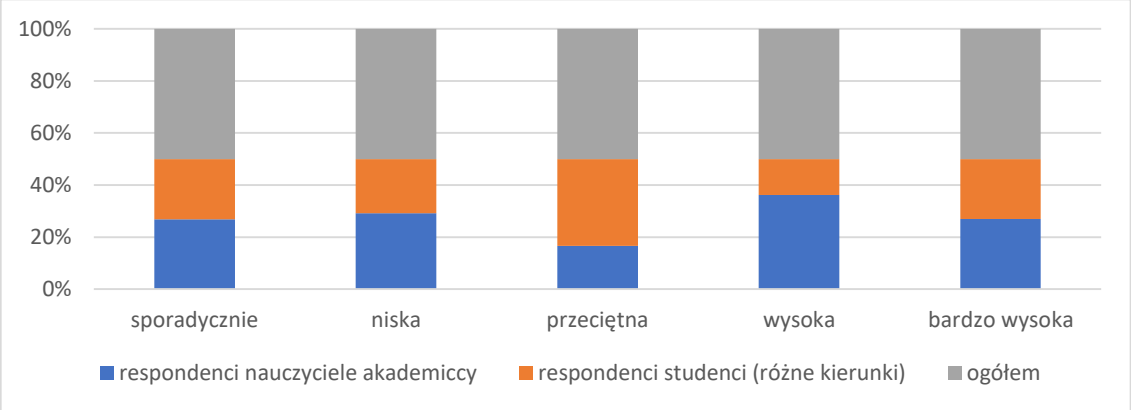
Źródło: opracowanie własne na podstawie badań własnych

W badaniu wzięło udział 500 osób zatrudnionych na stanowisku, nauczycieli akademickich oraz 500 osób studiujących w uczelni wyższej. Z przeprowadzonej analizy wynika, że nauczyciele akademiccy jak i studenci (różne kierunki) ocenili brak dostępu do Internetu w uczelni wyższej w stopniu niskim i przeciętnym. Wskazuje na to 156 respondentów, co w udziale procentowym wynosi 31,2% dla nauczycieli akademickich i 236 respondentów, co w udziale procentowym dla studentów wynosi 47,2%.

Analizując udzielone odpowiedzi w opinii 34 respondentów, co w udziale procentowym wynosi 6,8% dla nauczycieli akademickich i 29 respondentów, co w udziale procentowym daje 5,8% dla studentów (różne kierunki) świadczy, że pojawienie się braku dostępu do Internetu stanowi bardzo duże zagrożenie dla systemu informacyjnego uczelni wyższej.

Wykres 3.111. przedstawia odpowiedzi respondentów grupy nauczyciele akademiccy i grupy studenci (różne kierunki) na temat braku dostępu do Internetu w uczelni wyższej.

Wykres 3.111. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy studenci (różne kierunki) na temat stopnia zagrożenia systemu uczelni wyższej przez braku dostępu do Internetu



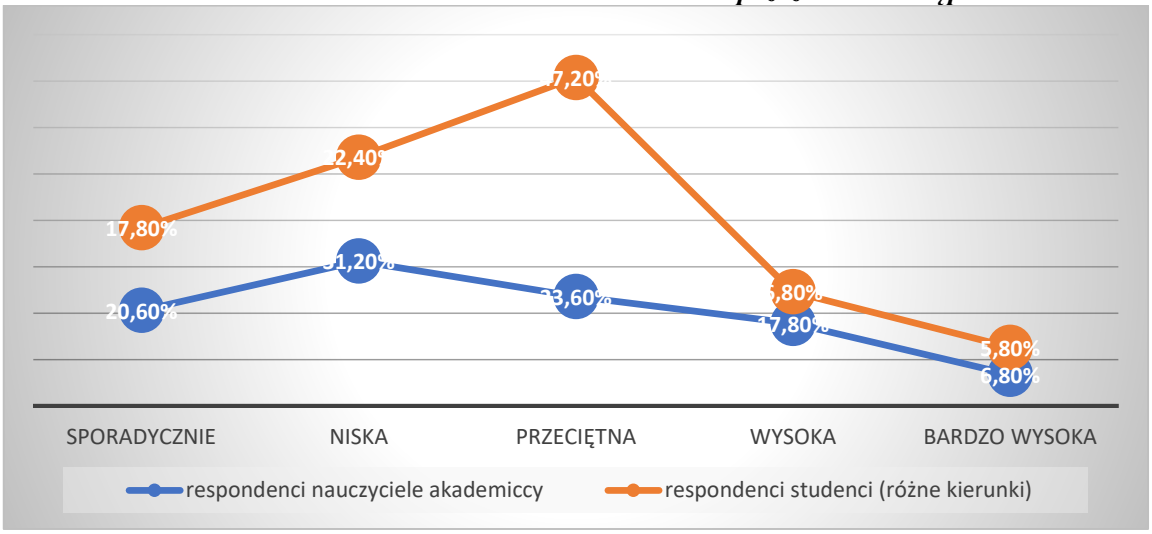
Źródło: opracowanie własne na podstawie badań własnych

O stopniu zależności świadczy współczynnik korelacji liniowej Pearsona na poziomie 0,57 i współczynnik determinacji liniowej, który wskazuje procent wyjaśnionej liniowo zmienności równy 32,49%. Wykres 3.112. pokazuje zależność między respondentami grupy nauczyciele akademiccy i grupy studenci (różne kierunki) pod względem stopnia zagrożenia systemu uczelni wyższej przez brak dostępu do Internetu.

$$r_{xy} = \frac{\frac{1}{n}\sum_{i=1}^{n}(x_i-\bar{x})(y_i-\bar{y})}{S_x S_y}=0{,}57$$

$$\mathrm{WD}=r_{xy}^{2} * 100\% = 32{,}49\%$$

Wykres 3.112. Zależność między respondentami grupy nauczyciele akademiccy i grupy studenci (różne kierunki) pod względem stopnia zagrożenia systemu uczelni wyższej przez braku dostępu do Internetu



Źródło: opracowanie własne na podstawie badań własnych

W związku z faktem, że wartość liczbowa w ocenie relacji jest dodatnia oznacza to, iż wraz ze wzrostem wartości jednej zmiennej rosną wartości także drugiej. Tabela 3.57. przedstawia odpowiedzi respondentów grupy kadra administracyjna i grupy studenci (różne kierunki) na temat zagrożeń systemu informacyjnego w uczelni wyższej przez braku dostępu do Internetu.

Tabela 84 Tabela 3.57. Odpowiedzi respondentów grupy kadra administracyjna i grupy studenci (różne kierunki) na temat braku dostępu do Internetu w uczelni wyższej

Odpowiedzi badanych osób brak dostępu do Internetu						
Osoby poddane badaniu	**Respondenci kadra administracyjna**		**Respondenci studenci (różne kierunki)**		**OGÓŁEM**	
Ocena	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***
sporadycznie	76	15,2%	89	17,8%	165	16,5%
niska	102	20,4%	112	22,4%	214	21,4%
przeciętna	269	53,8%	236	47,2%	505	50,5%
wysoka	36	7,2%	34	6,8%	70	7%
bardzo wysoka	17	3,4%	29	5,8%	46	4,6%
	500	**100%**	**500**	**100%**	**1000**	**100%**

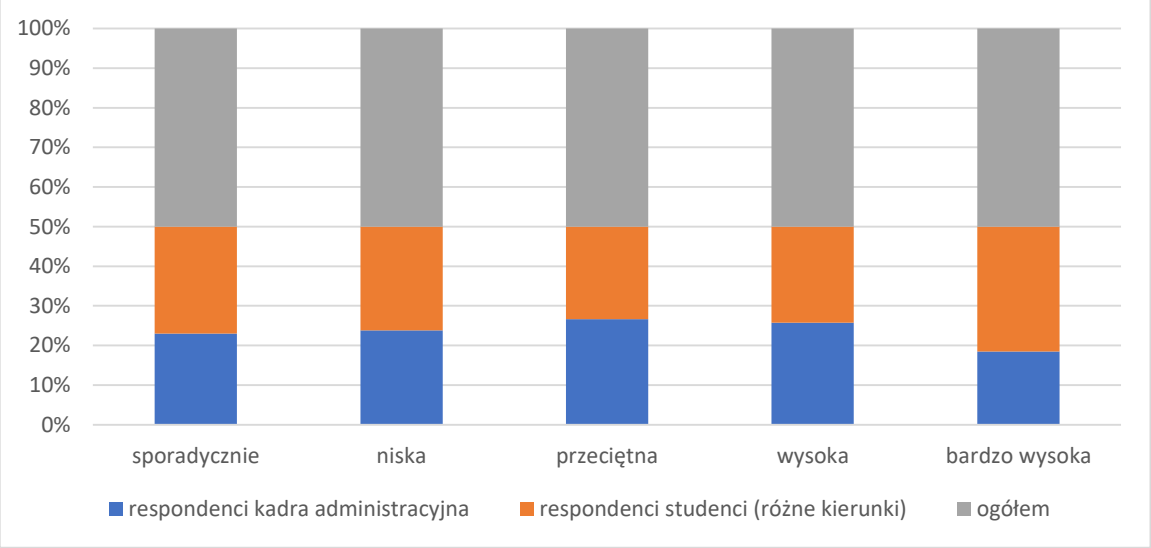
Źródło: opracowanie własne na podstawie badań własnych

W badaniu wzięło udział 500 osób zatrudnionych na stanowisku, kadra administracyjna oraz 500 osób studiujących na uczelni wyższej. Z przeprowadzonej analizy wynika, że kadra administracyjna jak i studenci (różne kierunki) ocenili brak dostępu do Internetu w uczelni wyższej w stopniu przeciętnym. Wskazuje na to 269 respondentów,

co w udziale procentowym wynosi 53,8% dla kadry administracyjnej i 236 respondentów, co w udziale procentowym dla studentów (różne roczniki) wynosi 47,2%.

Analizując udzielone odpowiedzi w opinii 17 respondentów, co w udziale procentowym wynosi 3,4% dla kadry administracyjnej i 29 respondentów, co w udziale procentowym daje 5,8% dla studentów (różne roczniki) świadczy, że pojawienie się braku dostępu do Internetu stanowi bardzo duże zagrożenie dla systemu informacyjnego uczelni wyższej. Wykres 3.113. przedstawia odpowiedzi respondentów grupy kadra administracyjna i grupy studenci (różne kierunki) na temat braku dostępu do Internetu w uczelni wyższej.

Wykres 3.113. Odpowiedzi respondentów grupy kadra administracyjna i grupy studenci (różne kierunki) na temat stopnia zagrożenia systemu uczelni wyższej przez braku dostępu do Internetu



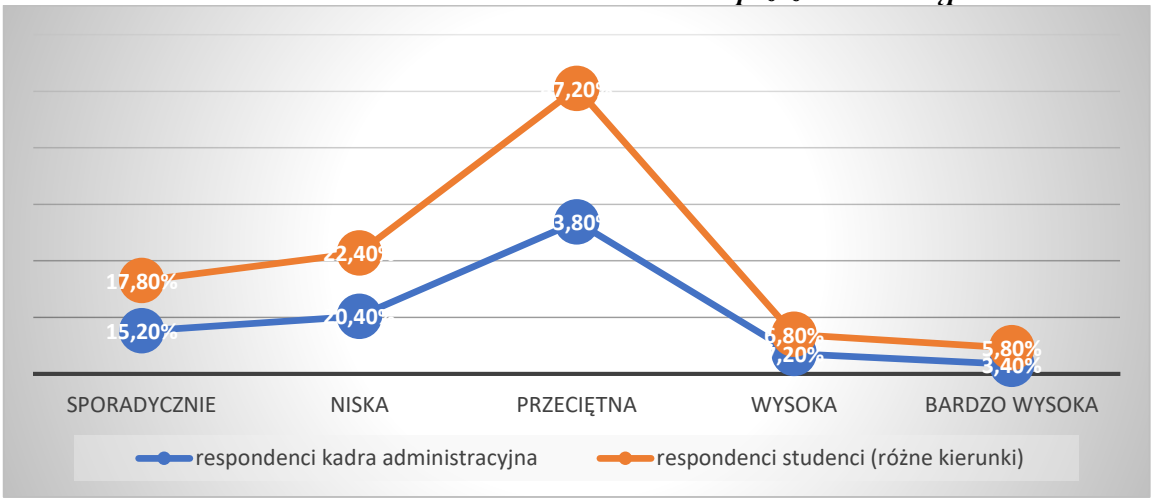
Źródło: opracowanie własne na podstawie badań własnych

O stopniu zależności świadczy współczynnik korelacji liniowej Pearsona na poziomie 0,99 i współczynnik determinacji liniowej, który wskazuje procent wyjaśnionej liniowo zmienności równy 98,01%. Wykres 3.114. pokazuje zależność między respondentami grupy kadra administracyjna i grupy studenci (różne kierunki) pod względem stopnia zagrożenia systemu uczelni wyższej przez brak dostępu do Internetu.

$$r_{xy} = \frac{\frac{1}{n}\sum_{i=1}^{n}(x_i-\bar{x})(y_i-\bar{y})}{S_x S_y}=0{,}99$$

$$\mathrm{WD}=r\frac{2}{xy} * 100\% = 98{,}01\%$$

Wykres 3.114. Zależność między respondentami grupy kadra administracyjna i grupy studenci (różne kierunki) pod względem stopnia zagrożenia systemu uczelni wyższej przez braku dostępu do Internetu



Źródło: opracowanie własne na podstawie badań własnych

W związku z faktem, że wartość liczbowa w ocenie relacji jest dodatnia oznacza to, iż wraz ze wzrostem wartości jednej zmiennej rosną wartości także drugiej.

16. Co Państwa zdaniem jest najczęstszym problemem w sprawnym działaniu systemu w uczelni wyższej?

b) Modernizacja systemu przez moderatora

Rozkład odpowiedzi respondentów grupy nauczyciele akademiccy i grupy kadra administracyjna dotyczący oceny przez użytkowników stopnia problemów związanych z modernizacją systemu przez moderatora w uczelni wyższej prezentuje tabela 3.58.

Tabela 3.58. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy kadra administracyjna na temat problemów związanych z modernizacją systemu w uczelni wyższej

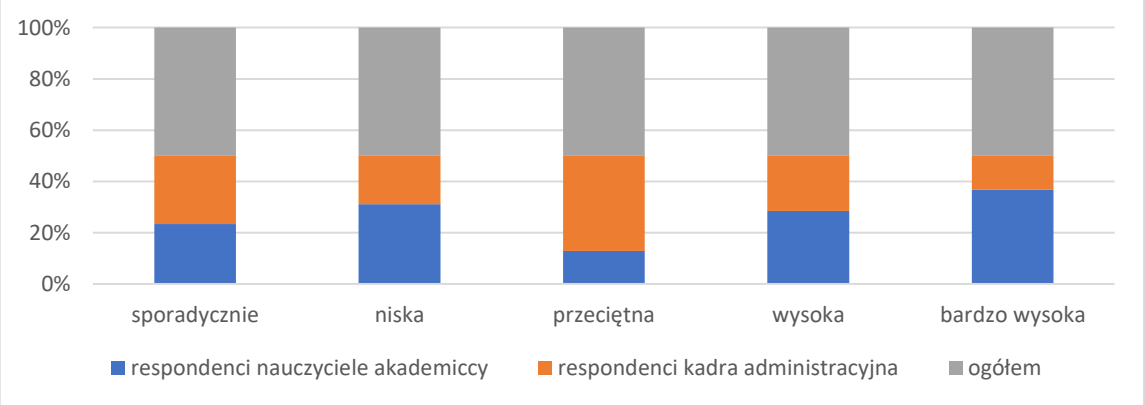
Odpowiedzi badanych osób modernizacja systemu przez moderatora						
Osoby poddane badaniu	**Respondenci nauczyciele akademiccy**		**Respondenci kadra administracyjna**		**OGÓŁEM**	
Ocena	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***
sporadycznie	78	15,6%	89	17,8%	167	16,7%
niska	312	62,4%	189	37,8%	501	50,1%
przeciętna	68	13,6%	196	39,2%	264	26,4%
wysoka	28	5,6%	21	4,2%	49	4,9%
bardzo wysoka	14	2,8%	5	1%	19	1,9%
	500	**100%**	**500**	**100%**	**1000**	**100%**

Źródło: opracowanie własne na podstawie badań własnych

W badaniu wzięło udział 500 osób zatrudnionych na stanowisku, nauczycieli akademickich oraz 500 osób zatrudnionych na stanowisku kadry administracyjnej. Z przeprowadzonej analizy wynika, że nauczyciele akademiccy jak i kadra administracyjna ocenili modernizację systemu w uczelni wyższej w stopniu niskim i przeciętnym. Wskazuje na to 312 respondentów, co w udziale procentowym wynosi 62,04% dla nauczycieli akademickich i 196 respondentów, co w udziale procentowym dla kadry administracyjnej wynosi 39,2%.

Analizując udzielone odpowiedzi w opinii 14 respondentów, co w udziale procentowym wynosi 2,8% dla nauczycieli akademickich i 5 respondentów, co w udziale procentowym daje 1% dla kadry administracyjnej świadczy, że pojawienie się modernizacji systemu stanowi bardzo duże zagrożenie dla systemu informacyjnego uczelni wyższej. Wykres 3.115. przedstawia odpowiedzi respondentów grupy nauczyciele akademiccy i grupy kadra administracyjna na temat modernizacji systemu w uczelni wyższej.

Wykres 3.115. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy kadra administracyjna na temat stopnia zagrożenia systemu uczelni wyższej przez modernizację systemu



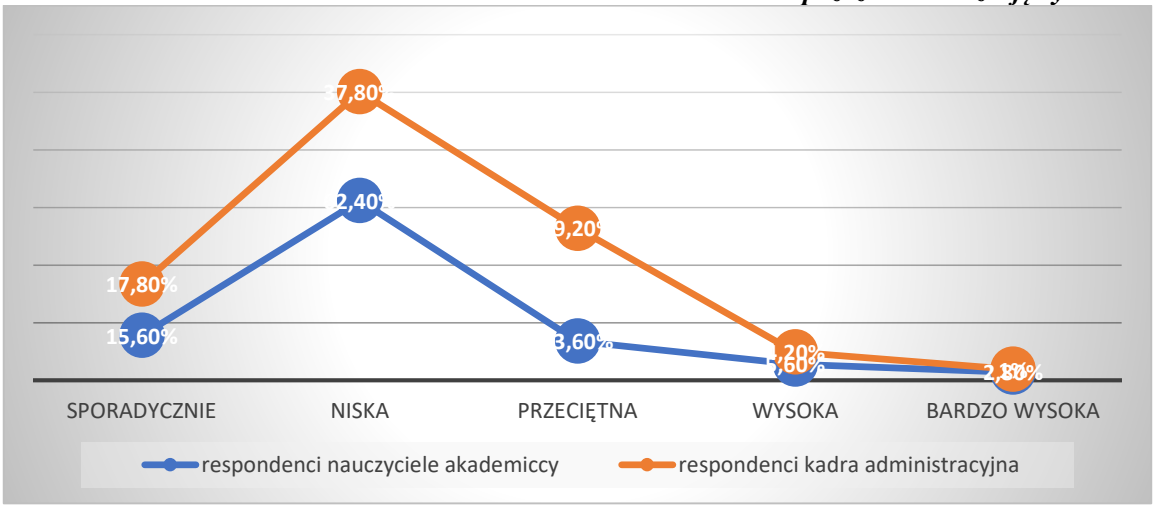
Źródło: opracowanie własne na podstawie badań własnych

O stopniu zależności świadczy współczynnik korelacji liniowej Pearsona na poziomie 0,68 i współczynnik determinacji liniowej, który wskazuje procent wyjaśnionej liniowo zmienności równy 46,24%. Wykres 3.116. pokazuje zależność między respondentami grupy nauczyciele akademiccy i grupy kadra administracyjna pod względem stopnia zagrożenia systemu uczelni wyższej przez modernizację systemu.

$$r_{xy} = \frac{\frac{1}{n}\sum_{i=1}^{n}(x_i-\bar{x})(y_i-\bar{y})}{S_x S_y}=0{,}68$$

$$\mathrm{WD}=r_{xy}^{2} * 100\% = 46{,}24\%$$

Wykres 3.116. Zależność między respondentami grupy nauczyciele akademiccy i grupy kadra administracyjna pod względem stopnia zagrożenia systemu uczelni wyższej przez modernizację systemu



Źródło: opracowanie własne na podstawie badań własnych

W związku z faktem, że wartość liczbowa w ocenie relacji jest dodatnia oznacza to, iż wraz ze wzrostem wartości jednej zmiennej rosną wartości także drugiej. Tabela 3.59. przedstawia odpowiedzi respondentów grupy nauczyciele akademiccy i grupy studenci (różne kierunki) na temat zagrożeń systemu informacyjnego w uczelni wyższej przez modernizację systemu.

Tabela 3.59. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy studenci (różne kierunki) na temat problemów związanych z modernizacją systemu w uczelni wyższej

Odpowiedzi badanych osób modernizacja systemu przez moderatora						
Osoby poddane badaniu	**Respondenci nauczyciele akademiccy**		**Respondenci studenci (różne kierunki)**		**OGÓŁEM**	
Ocena	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***
sporadycznie	78	15,6%	136	27,2%	214	21,4%
niska	312	62,4%	164	32,8%	476	47,6%
przeciętna	68	13,6%	158	31,6%	226	22,6%
wysoka	28	5,6%	31	6,2%	59	5,9%
bardzo wysoka	14	2,8%	11	2,2%	25	2,5%
	500	**100%**	**500**	**100%**	**1000**	**100%**

Źródło: opracowanie własne na podstawie badań własnych

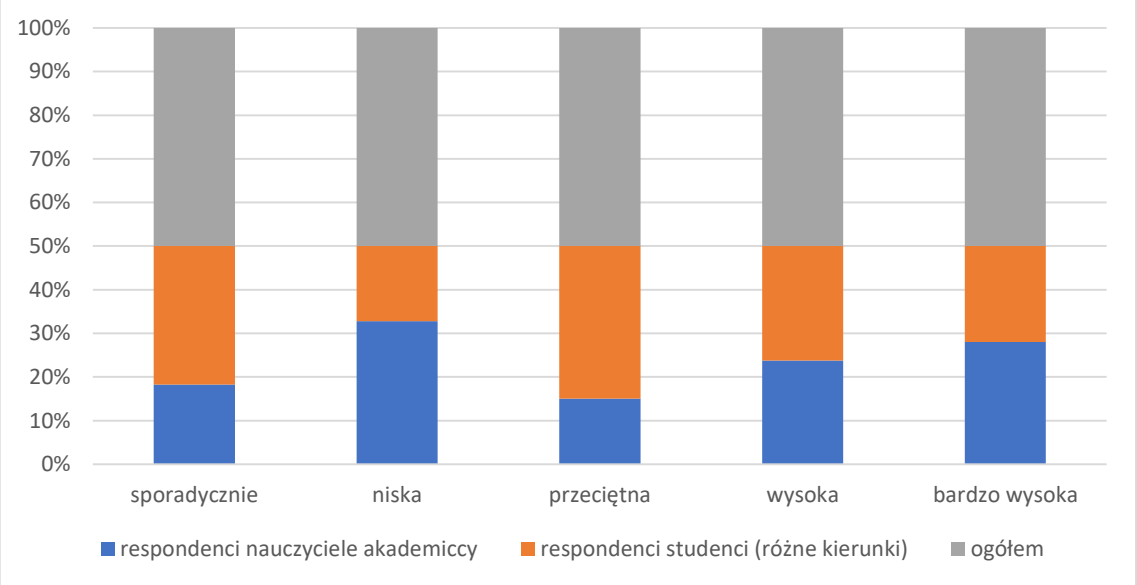
W badaniu wzięło udział 500 osób zatrudnionych na stanowisku, nauczycieli akademickich oraz 500 osób studiujących w uczelni wyższej. Z przeprowadzonej analizy wynika, że nauczyciele akademiccy jak i studenci (różne kierunki) ocenili modernizację systemu w uczelni wyższej w stopniu niskim. Wskazuje na to 312 respondentów, co

w udziale procentowym wynosi 62,4% dla nauczycieli akademickich i 164 respondentów, co w udziale procentowym dla studentów (różne kierunki) wynosi 32,8%.

Analizując udzielone odpowiedzi w opinii 14 respondentów, co w udziale procentowym wynosi 2,8% dla nauczycieli akademickich i 11 respondentów, co w udziale procentowym daje 2,2% dla studentów (różnych kierunków) świadczy, że pojawienie się modernizacji systemu stanowi bardzo duże zagrożenie dla systemu informacyjnego uczelni wyższej.

Wykres 3.117. przedstawia odpowiedzi respondentów grupy nauczyciele akademiccy i grupy studenci (różne kierunki) na temat modernizacji systemu w uczelni wyższej.

Wykres 3.117. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy studenci (różne kierunki) na temat stopnia zagrożenia systemu uczelni wyższej przez modernizację systemu



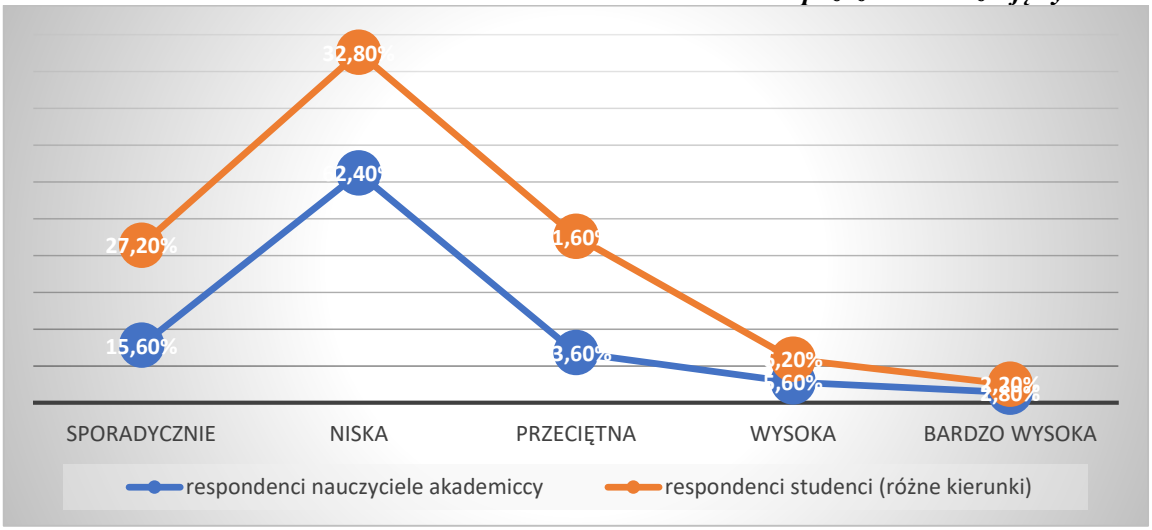
Źródło: opracowanie własne na podstawie badań własnych

O stopniu zależności świadczy współczynnik korelacji liniowej Pearsona na poziomie 0,66 i współczynnik determinacji liniowej, który wskazuje procent wyjaśnionej liniowo zmienności równy 43,56%. Wykres 3.118. pokazuje zależność między respondentami grupy nauczyciele akademiccy i grupy studenci pod względem stopnia zagrożenia systemu uczelni wyższej przez modernizację systemu.

$$r_{xy} = \frac{\frac{1}{n}\sum_{i=1}^{n}(x_i-\bar{x})(y_i-\bar{y})}{S_x S_y}=0{,}66$$

$$\mathrm{WD}=r_{xy}^{2} * 100\% = 43{,}56\%$$

Wykres 3.118. Zależność między respondentami grupy nauczyciele akademiccy i grupy studenci (różne kierunki) pod względem stopnia zagrożenia systemu uczelni wyższej przez modernizację systemu



Źródło: opracowanie własne na podstawie badań własnych

W związku z faktem, że wartość liczbowa w ocenie relacji jest dodatnia oznacza to, iż wraz ze wzrostem wartości jednej zmiennej rosną wartości także drugiej. Tabela 3.60. przedstawia odpowiedzi respondentów grupy kadra administracyjna i grupy studenci (różne kierunki) na temat zagrożeń systemu informacyjnego w uczelni wyższej przez modernizację systemu.

Tabela 3.60. Odpowiedzi respondentów grupy kadra administracyjna i grupy studenci (różne kierunki) na temat problemów związanych z modernizacją systemu w uczelni wyższej

Odpowiedzi badanych osób modernizacja systemu przez moderatora						
Osoby poddane badaniu	**Respondenci kadra administracyjna**		**Respondenci studenci (różne kierunki)**		**OGÓŁEM**	
Ocena	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***
sporadycznie	89	17,8%	136	27,2%	225	22,5%
niska	189	37,8%	164	32,8%	353	35,3%
przeciętna	196	39,2%	158	31,6%	354	35,4%
wysoka	21	4,2%	31	6,2%	52	5,2%
bardzo wysoka	5	1%	11	2,2%	16	1,6%
	500	**100%**	**500**	**100%**	**1000**	**100%**

Źródło: opracowanie własne na podstawie badań własnych

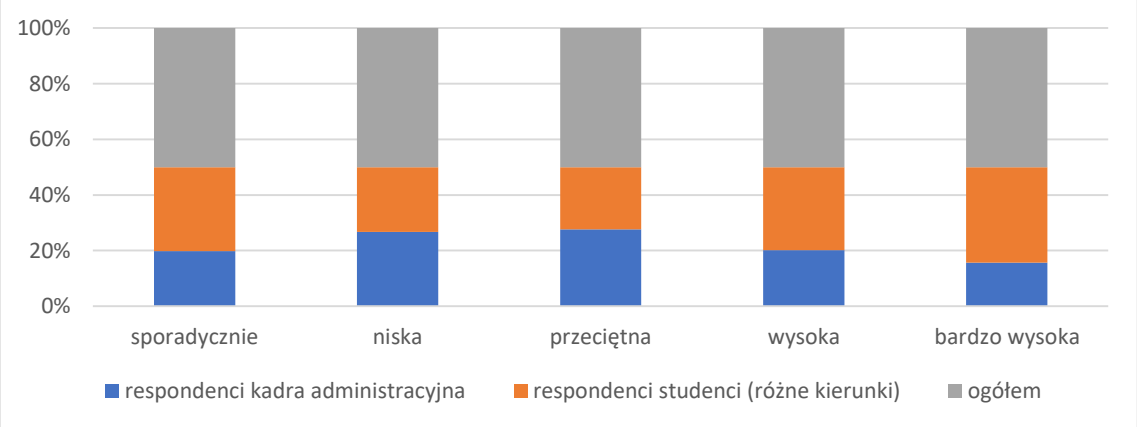
W badaniu wzięło udział 500 osób zatrudnionych na stanowisku, kadra administracyjna oraz 500 osób studiujących w uczelni wyższej. Z przeprowadzonej analizy wynika, że kadra administracyjna jak i studenci (różne kierunki) ocenili modernizację sys-

temu w uczelni wyższej w stopniu przeciętnym i niskim. Wskazuje na to 196 respondentów, co w udziale procentowym wynosi 39,2% dla kadry administracyjnej i 164 respondentów, co w udziale procentowym dla studentów (różnych roczników) wynosi 32,8%.

Analizując udzielone odpowiedzi w opinii 5 respondentów, co w udziale procentowym wynosi 1% dla kadry administracyjnej i 11 respondentów, co w udziale procentowym daje 2,2% dla studentów (różnych kierunków) świadczy, że pojawienie się modernizacji systemu stanowi bardzo duże zagrożenie dla systemu informacyjnego uczelni wyższej.

Wykres 3.119 przedstawia odpowiedzi respondentów grupy kadra administracyjna i grupy studenci (różne kierunki) na temat modernizacji systemu w uczelni wyższej.

Wykres 3.119. Odpowiedzi respondentów grupy kadra administracyjna i grupy studenci (różne kierunki) na temat stopnia zagrożenia systemu uczelni wyższej przez modernizację systemu



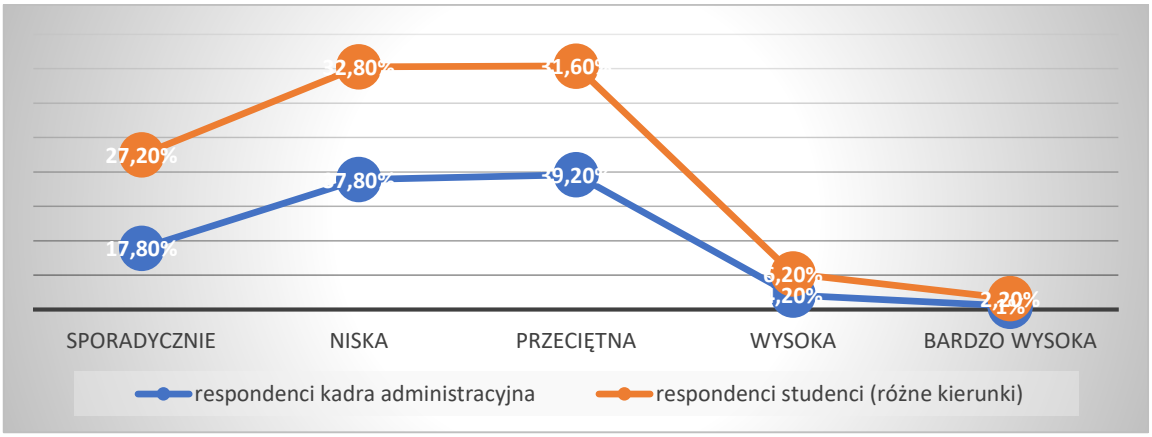
Źródło: opracowanie własne na podstawie badań własnych

O stopniu zależności świadczy współczynnik korelacji liniowej Pearsona na poziomie 0,94 i współczynnik determinacji liniowej, który wskazuje procent wyjaśnionej liniowo zmienności równy 88,36%. Wykres 3.120. pokazuje zależność między respondentami grupy kadra administracyjna i grupy studenci (różne kierunki) pod względem stopnia zagrożenia systemu uczelni wyższej przez modernizację systemu.

$$r_{xy} = \frac{\frac{1}{n}\sum_{i=1}^{n}(x_i-\bar{x})(y_i-\bar{y})}{S_x S_y}=0{,}94$$

$$\mathrm{WD}=r_{xy}^{2} * 100\% = 88{,}36\%$$

Wykres 3.120 Zależność między respondentami grupy kadra administracyjna i grupy studenci (różne kierunki) pod względem stopnia zagrożenia systemu uczelni wyższej przez modernizację systemu



Źródło: opracowanie własne na podstawie badań własnych

W związku z faktem, że wartość liczbowa w ocenie relacji jest dodatnia oznacza to, iż wraz ze wzrostem wartości jednej zmiennej rosną wartości także drugiej.

16. Co Państwa zdaniem jest najczęstszym problemem w sprawnym działaniu systemu w uczelni wyższej?

c) Awaria systemu

Rozkład odpowiedzi respondentów grupy nauczyciele akademiccy i grupy kadra administracyjna dotyczący oceny przez użytkowników stopnia problemów związanych z awarią systemu w uczelni wyższej prezentuje tabela 3.61.

Tabela 3.61. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy kadra administracyjna na temat problemów związanych z awarią systemów w uczelni wyższej

Odpowiedzi badanych osób awaria systemów						
Osoby poddane badaniu	**Respondenci nauczyciele akademiccy**		**Respondenci kadra administracyjna**		**OGÓŁEM**	
Ocena	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***
sporadycznie	80	16%	89	17,8%	169	16,9%
niska	114	22,8%	105	21%	219	21,9%
przeciętna	228	45,6%	268	53,6%	496	49,6%
wysoka	69	13,8%	31	6,2%	100	10%
bardzo wysoka	9	1,8%	7	1,4%	16	1,6%
	500	**100%**	**500**	**100%**	**1000**	**100%**

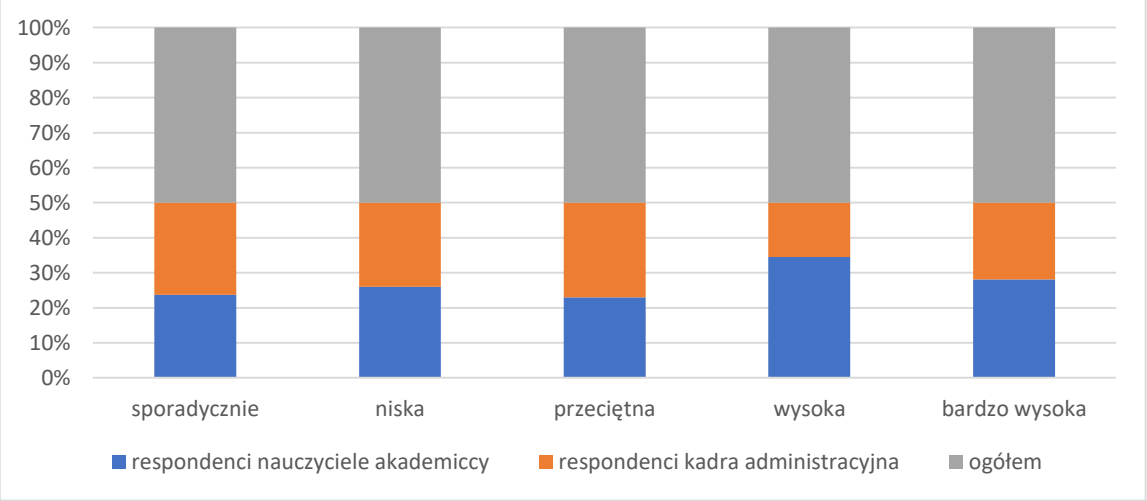
Źródło: opracowanie własne na podstawie badań własnych

W badaniu wzięło udział 500 osób zatrudnionych na stanowisku, nauczycieli akademickich oraz 500 osób zatrudnionych na stanowisku kadry administracyjnej. Z przeprowadzonej analizy wynika, że nauczyciele akademiccy jak i kadra administracyjna ocenili awarię systemu w uczelni wyższej w stopniu przeciętnym. Wskazuje na to 228 respondentów, co w udziale procentowym wynosi 45,6% dla nauczycieli akademickich i 268 respondentów, co w udziale procentowym dla kadry administracyjnej wynosi 53,6%.

Analizując udzielone odpowiedzi w opinii 9 respondentów, co w udziale procentowym wynosi 1,8% dla nauczycieli akademickich i 7 respondentów, co w udziale procentowym daje 1,4% dla kadry administracyjnej świadczy, że pojawienie się awarii systemu stanowi bardzo duże zagrożenie dla systemu informacyjnego uczelni wyższej.

Wykres 3.121. przedstawia odpowiedzi respondentów grupy nauczyciele akademiccy i grupy kadra administracyjna na temat awarii systemu w uczelni wyższej.

Wykres 3.121. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy kadra administracyjna na temat stopnia zagrożenia systemu uczelni wyższej przez awarię systemu



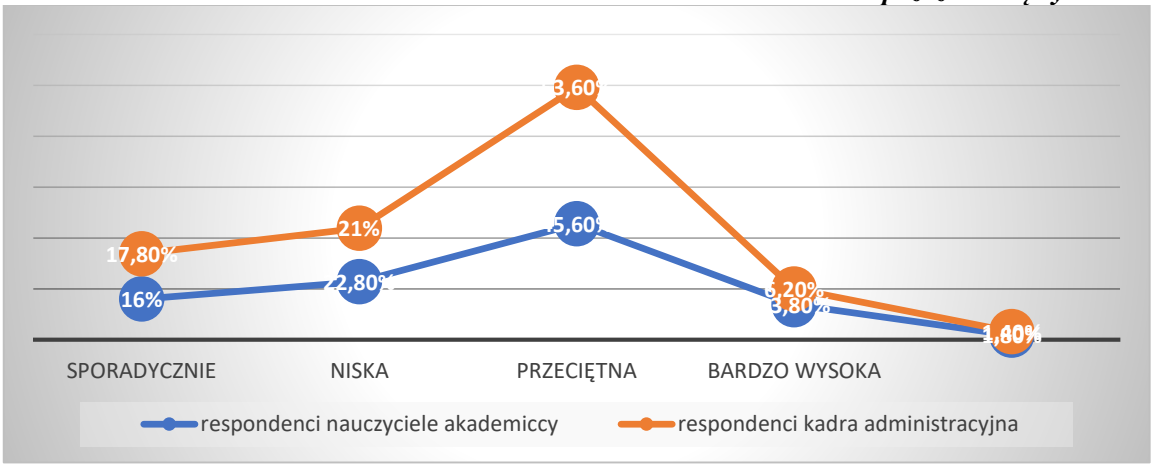
Źródło: opracowanie własne na podstawie badań własnych

O stopniu zależności świadczy współczynnik korelacji liniowej Pearsona na poziomie 0,98 i współczynnik determinacji liniowej, który wskazuje procent wyjaśnionej liniowo zmienności równy 96,04%. Wykres 3.122. pokazuje zależność między respondentami grupy nauczyciele akademiccy i grupy kadra administracyjna pod względem stopnia zagrożenia systemu uczelni wyższej przez awarię systemu.

$$r_{xy} = \frac{\frac{1}{n}\sum_{i=1}^{n}(x_i-\bar{x})(y_i-\bar{y})}{S_x S_y}=0{,}98$$

$$WD=r\frac{2}{xy} * 100\% = 96,4\%$$

Wykres 122. Zależność między respondentami grupy nauczyciele akademiccy i grupy kadra administracyjna pod względem stopnia zagrożenia systemu uczelni wyższej przez awarię systemu



Źródło: opracowanie własne na podstawie badań własnych

W związku z faktem, że wartość liczbowa w ocenie relacji jest dodatnia oznacza to, iż wraz ze wzrostem wartości jednej zmiennej rosną wartości także drugiej. Tabela 3.62. przedstawia odpowiedzi respondentów grupy nauczyciele akademiccy i grupy studenci (różne kierunki) na temat zagrożeń systemu informacyjnego w uczelni wyższej przez awarię systemu.

Tabela 3.62. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy studenci (różne kierunki) na temat problemów związanych z awarią systemu

Odpowiedzi badanych osób awaria systemów						
Osoby poddane badaniu	**Respondenci nauczyciele akademiccy**		**Respondenci studenci (różne kierunki)**		**OGÓŁEM**	
Ocena	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***
sporadycznie	80	16%	89	17,8%	169	16,9%
niska	114	22,8%	159	31,8%	273	27,3%
przeciętna	228	45,6%	198	39,6%	426	42,6%
wysoka	69	13,8%	42	8,4%	111	11,1%
bardzo wysoka	9	1,8%	12	2,4%	21	2,1%
	500	**100%**	**500**	**100%**	**1000**	**100%**

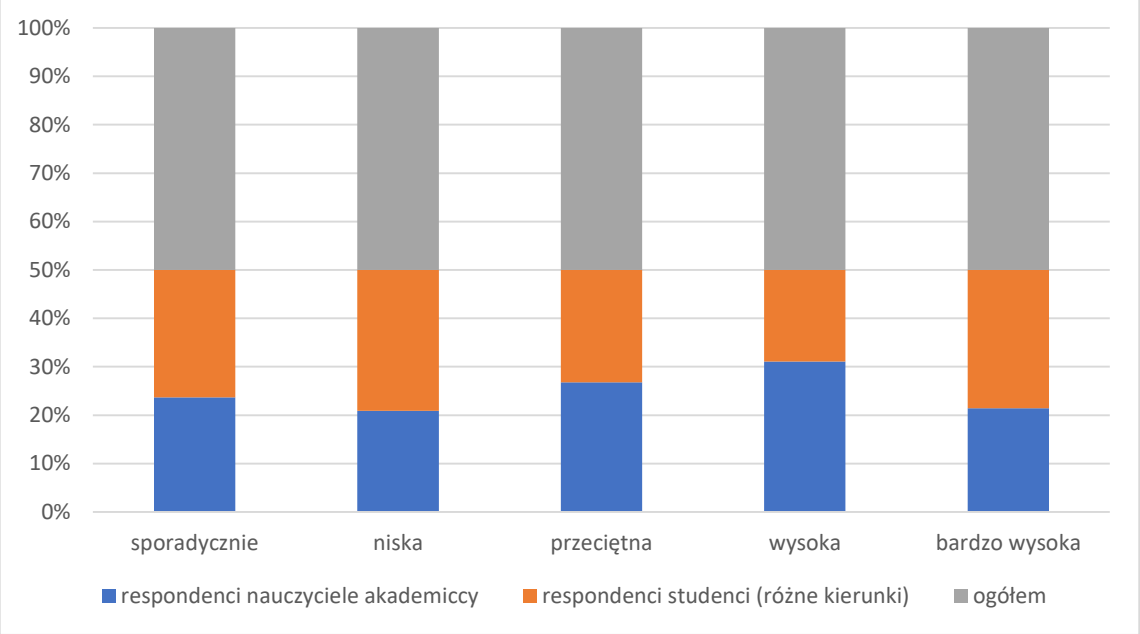
Źródło: opracowanie własne na podstawie badań własnych

W badaniu wzięło udział 500 osób zatrudnionych na stanowisku, nauczycieli akademickich oraz 500 osób studiujących na uczelni wyższej. Z przeprowadzonej analizy wynika, że nauczyciele akademiccy jak i studenci (różne kierunki) ocenili awarię systemu

w uczelni wyższej w stopniu przeciętnym. Wskazuje na to 228 respondentów, co w udziale procentowym wynosi 45,6% dla nauczycieli akademickich i 198 respondentów, co w udziale procentowym dla studentów wynosi 39,6%.

Analizując udzielone odpowiedzi w opinii 9 respondentów, co w udziale procentowym wynosi 1,8% dla nauczycieli akademickich i 12 respondentów, co w udziale procentowym daje 2,4% dla studentów świadczy, że pojawienie się awarii systemu stanowi bardzo duże zagrożenie dla systemu informacyjnego uczelni wyższej. Wykres 3.123. przedstawia odpowiedzi respondentów grupy nauczyciele akademiccy i grupy studentów na temat awarii systemu w uczelni wyższej.

Wykres 3.123. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy studenci (różne kierunki) na temat stopnia zagrożenia systemu uczelni wyższej przez awarię systemu



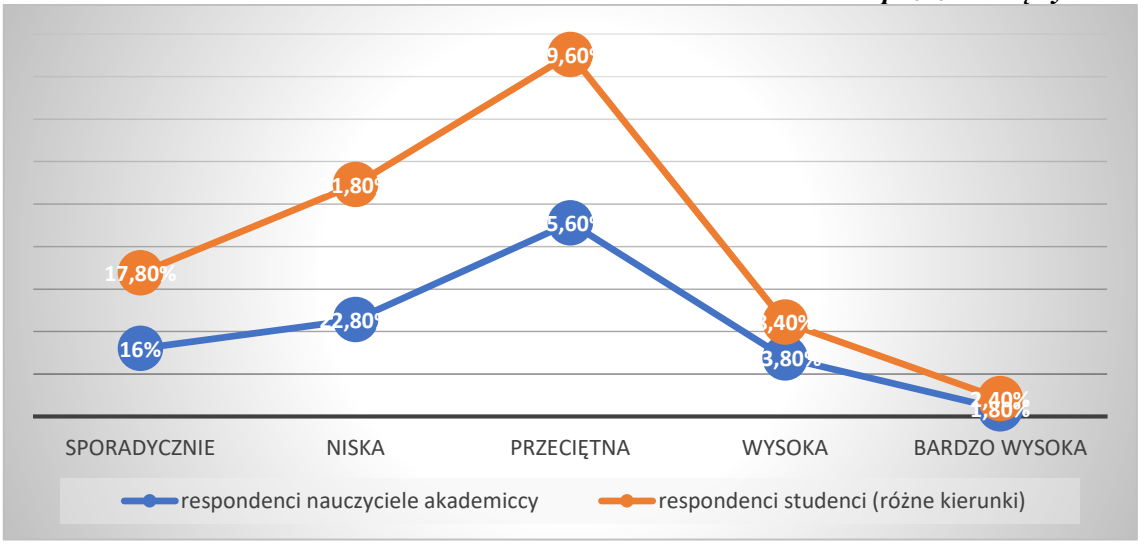
Źródło: opracowanie własne na podstawie badań własnych

O stopniu zależności świadczy współczynnik korelacji liniowej Pearsona na poziomie 0,93 i współczynnik determinacji liniowej, który wskazuje procent wyjaśnionej liniowo zmienności równy 86,49%. Wykres 3.124. pokazuje zależność między respondentami grupy nauczyciele akademiccy i grupy studenci (różne kierunki) pod względem stopnia zagrożenia systemu uczelni wyższej przez awarię systemu.

$$r_{xy} = \frac{\frac{1}{n}\sum_{i=1}^{n}(x_i-\bar{x})(y_i-\bar{y})}{S_x S_y}=0{,}93$$

$$WD=r\frac{2}{xy} * 100\% = 86{,}49\%$$

Wykres 3.124. Zależność między respondentami grupy nauczyciele akademiccy i grupy studenci (różne kierunki) pod względem stopnia zagrożenia systemu uczelni wyższej przez awarię systemu



Źródło: opracowanie własne na podstawie badań własnych

W związku z faktem, że wartość liczbowa w ocenie relacji jest dodatnia oznacza to, iż wraz ze wzrostem wartości jednej zmiennej rosną wartości także drugiej. Tabela 3.63. przedstawia odpowiedzi respondentów grupy kadra administracyjna i grupy studenci (różne kierunki) na temat zagrożeń systemu informacyjnego w uczelni wyższej przez awarię systemu.

Tabela 3.63. Odpowiedzi respondentów grupy kadra administracyjna i grupy studenci (różne kierunki) na temat problemów związanych z awarią systemu

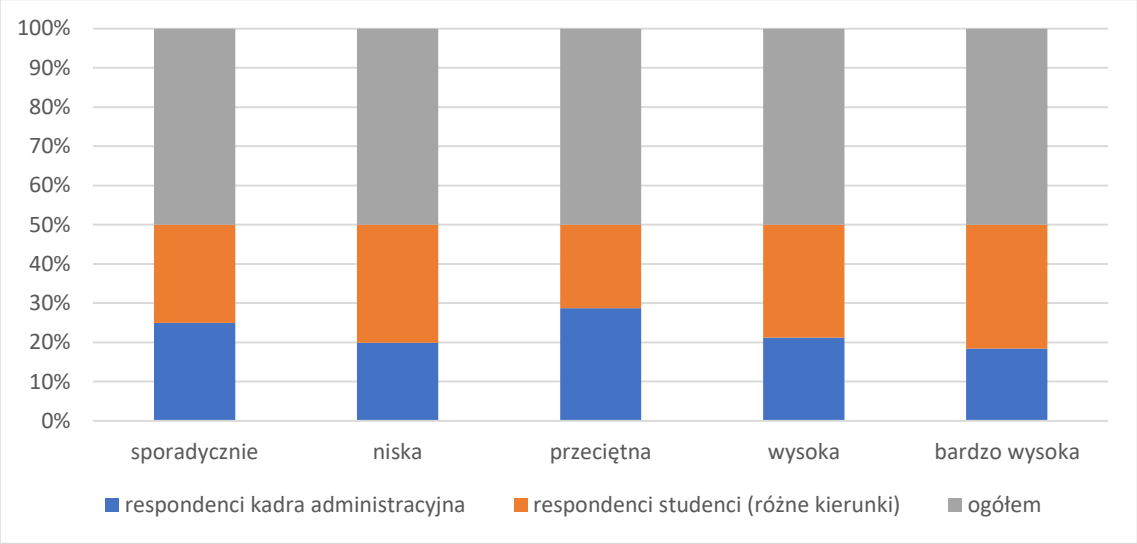
Odpowiedzi badanych osób awaria systemów						
Osoby poddane badaniu	**Respondenci kadra administracyjna**		**Respondenci studenci (różne kierunki)**		**OGÓŁEM**	
Ocena	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***
sporadycznie	89	17,8%	89	17,8%	178	17,8%
niska	105	21%	159	31,8%	264	26,4%
przeciętna	268	53,6%	198	39,6%	466	46,6%
wysoka	31	6,2%	42	8,4%	73	7,3%
bardzo wysoka	7	1,4%	12	2,4%	19	1,9%
	500	**100%**	**500**	**100%**	**1000**	**100%**

Źródło: opracowanie własne na podstawie badań własnych

W badaniu wzięło udział 500 osób zatrudnionych na stanowisku, kadra administracyjna oraz 500 osób studiujących w uczelni wyższej. Z przeprowadzonej analizy wynika, że kadra administracyjna jak i studenci ocenili awarię systemu w uczelni wyższej w stopniu przeciętnym. Wskazuje na to 268 respondentów, co w udziale procentowym wynosi 53,6% dla kadry administracyjnej 198 respondentów, co w udziale procentowym dla studentów wynosi 39,6%.

Analizując udzielone odpowiedzi w opinii 7 respondentów, co w udziale procentowym wynosi 1,4% dla kadry administracyjnej i 12 respondentów, co w udziale procentowym daje 2,4% dla studentów świadczy, że pojawienie się braku dostępu do Internetu stanowi bardzo duże zagrożenie dla systemu informacyjnego uczelni wyższej. Wykres 3.125. przedstawia odpowiedzi respondentów grupy kadra administracyjna i grupy studenci (różne kierunki) na temat awarii systemu w uczelni wyższej.

Wykres 3.125. Odpowiedzi respondentów grupy kadra administracyjna i grupy studenci (różne kierunki) na temat stopnia zagrożenia systemu uczelni wyższej przez awarię systemu



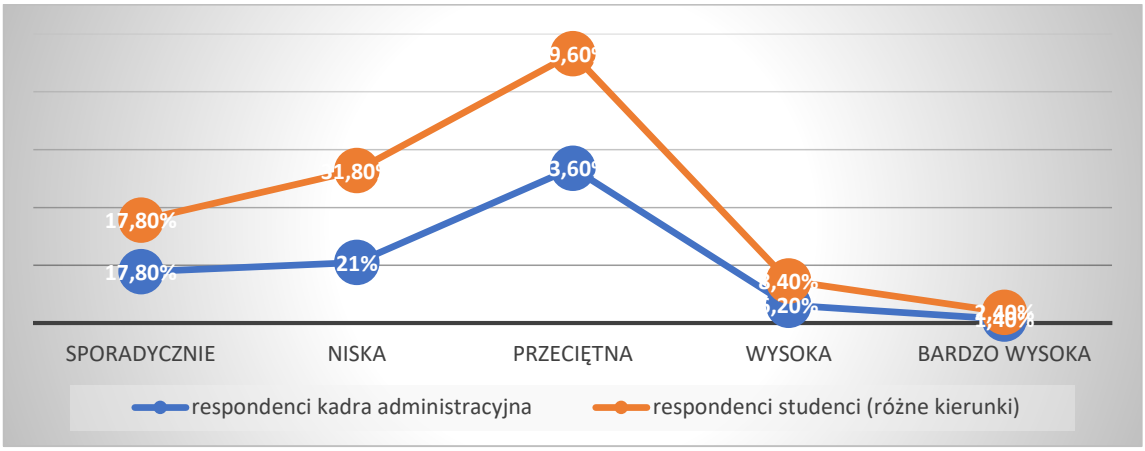
Źródło: opracowanie własne na podstawie badań własnych

O stopniu zależności świadczy współczynnik korelacji liniowej Pearsona na poziomie 0,91 i współczynnik determinacji liniowej, który wskazuje procent wyjaśnionej liniowo zmienności równy 82,81%. Wykres 3.126. pokazuje zależność między respondentami grupy kadra administracyjna i grupy studenci (różne kierunki) pod względem stopnia zagrożenia systemu uczelni wyższej przez awarię systemu.

$$r_{xy} = \frac{\frac{1}{n}\sum_{i=1}^{n}(x_i-\bar{x})(y_i-\bar{y})}{S_x S_y}=0{,}91$$

$$WD=r\frac{2}{xy} * 100\% = 82{,}81\%$$

Wykres 3.126. Zależność między respondentami grupy kadra administracyjna i grupy studenci (różne kierunki) pod względem stopnia zagrożenia systemu uczelni wyższej przez awarię systemu



Źródło: opracowanie własne na podstawie badań własnych

W związku z faktem, że wartość liczbowa w ocenie relacji jest dodatnia oznacza to, iż wraz ze wzrostem wartości jednej zmiennej rosną wartości także drugiej.

16. Co Państwa zdaniem jest najczęstszym problemem w sprawnym działaniu systemu w uczelni wyższej?

d) Przestarzałe oprogramowanie

Rozkład odpowiedzi respondentów grupy nauczyciele akademiccy i kadra administracyjna dotyczący oceny przez użytkowników stopnia problemów związanych z przestarzałym oprogramowaniem w uczelni wyższej prezentuje tabela 3.64.

Tabela 3.64. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy kadra administracyjna na temat przestarzałego oprogramowania

Odpowiedzi badanych osób przestarzałe oprogramowania						
Osoby poddane badaniu	**Respondenci nauczyciele akademiccy**		**Respondenci kadra administracyjna**		**OGÓŁEM**	
Ocena	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***
sporadycznie	12	2,4%	21	4,2%	33	3,3%
niska	42	8,4%	86	17,2%	128	12,8%
przeciętna	412	82,4%	358	71,6%	770	77%
wysoka	30	6%	29	5,8%	59	5,9%
bardzo wysoka	4	0,8%	6	1,2%	10	1%
	500	**100%**	**500**	**100%**	**1000**	**100%**

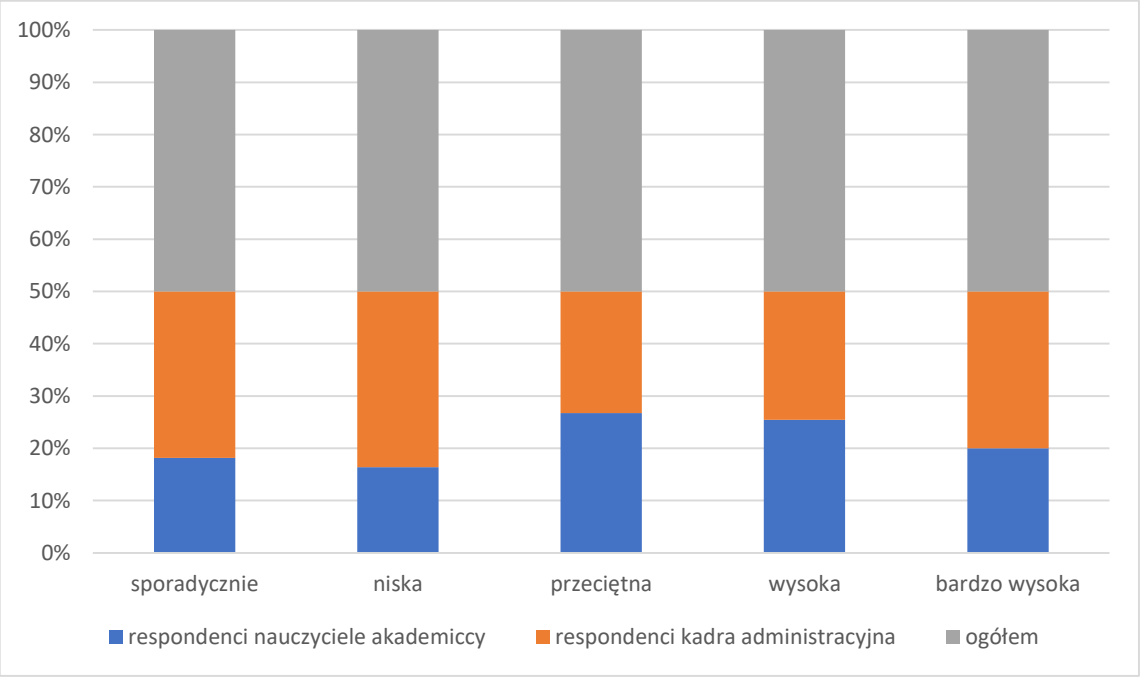
Źródło: opracowanie własne na podstawie badań własnych

W badaniu wzięło udział 500 osób zatrudnionych na stanowisku, nauczycieli akademickich oraz 500 osób zatrudnionych na stanowisku kadry administracyjnej. Z przeprowadzonej analizy wynika, że nauczyciele akademiccy jak i kadra administracyjna ocenili przestarzałe oprogramowania w uczelni wyższej w stopniu przeciętnym. Wskazuje na to 412 respondentów, co w udziale procentowym wynosi 82,4% dla nauczycieli akademickich i 358 respondentów, co w udziale procentowym dla kadry administracyjnej wynosi 71,6%.

Analizując udzielone odpowiedzi w opinii 4 respondentów, co w udziale procentowym wynosi 0,8% dla nauczycieli akademickich i 6 respondentów, co w udziale procentowym daje 1,2% dla kadry administracyjnej świadczy, że pojawienie się przestarzałego oprogramowania stanowi bardzo duże zagrożenie dla systemu informacyjnego uczelni wyższej.

Wykres 3.127. przedstawia odpowiedzi respondentów grupy nauczyciele akademiccy i grupy kadra administracyjna na temat przestarzałego oprogramowania w uczelni wyższej.

Wykres 3.127. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy kadra administracyjna na temat stopnia zagrożenia systemu uczelni wyższej przez przestarzałe oprogramowanie



Źródło: opracowanie własne na podstawie badań własnych

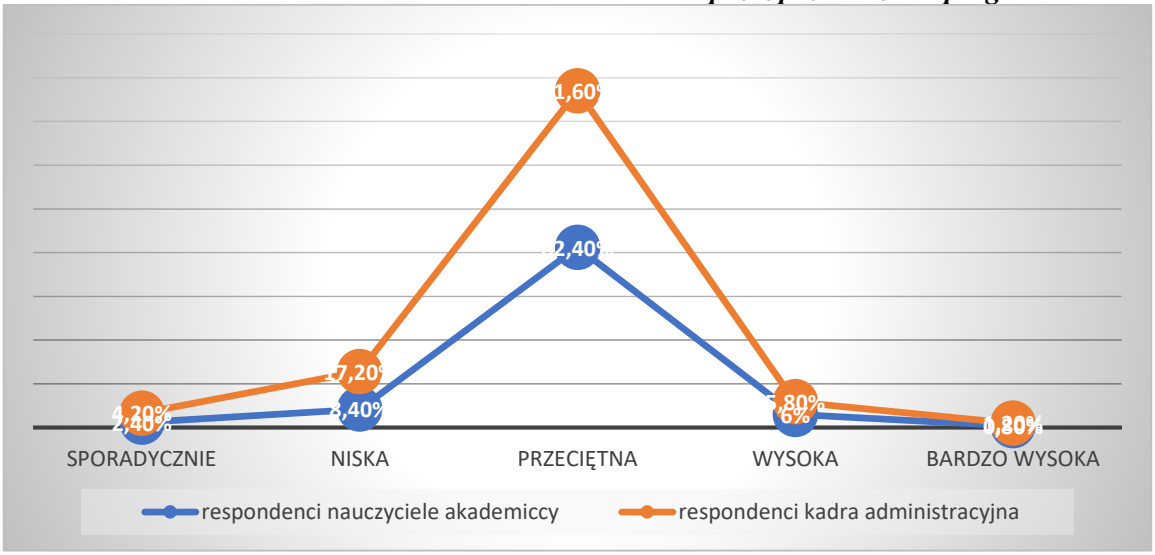
O stopniu zależności świadczy współczynnik korelacji liniowej Pearsona na poziomie 0,99 i współczynnik determinacji liniowej, który wskazuje procent wyjaśnionej liniowo zmienności równy 98,01%.

Wykres 3.128. pokazuje zależność między respondentami grupy nauczyciele akademiccy i grupy kadra administracyjna pod względem stopnia zagrożenia systemu uczelni wyższej przez przestarzałe oprogramowania.

$$r_{xy} = \frac{\frac{1}{n}\sum_{i=1}^{n}(x_i-\bar{x})(y_i-\bar{y})}{s_x s_y}=0{,}99$$

$$\mathrm{WD}=r_{xy}^{2} * 100\% = 98{,}1\%$$

Wykres 3.128. Zależność między respondentami grupy nauczyciele akademiccy i grupy kadry administracyjnej pod względem stopnia zagrożenia systemu uczelni wyższej przez przestarzałe oprogramowania



Źródło: opracowanie własne na podstawie badań własnych

W związku z faktem, że wartość liczbowa w ocenie relacji jest dodatnia oznacza to, iż wraz ze wzrostem wartości jednej zmiennej rosną wartości także drugiej. Tabela 3.65. przedstawia odpowiedzi respondentów grupy nauczyciele akademiccy i grupy studenci (różne kierunki) na temat zagrożeń systemu informacyjnego w uczelni wyższej na temat przestarzałego oprogramowania.

Tabela 3.65. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy studenci (różne kierunki) na temat przestarzałego oprogramowania

Odpowiedzi badanych osób przestarzałe oprogramowania						
Osoby poddane badaniu	**Respondenci nauczyciele akademiccy**		**Respondenci studenci (różne kierunki)**		**OGÓŁEM**	
Ocena	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***
sporadycznie	12	2,4%	69	13,8%	81	8,1%
niska	42	8,4%	196	39,2%	238	23,8%
przeciętna	412	82,4%	189	37,8%	601	60,1%

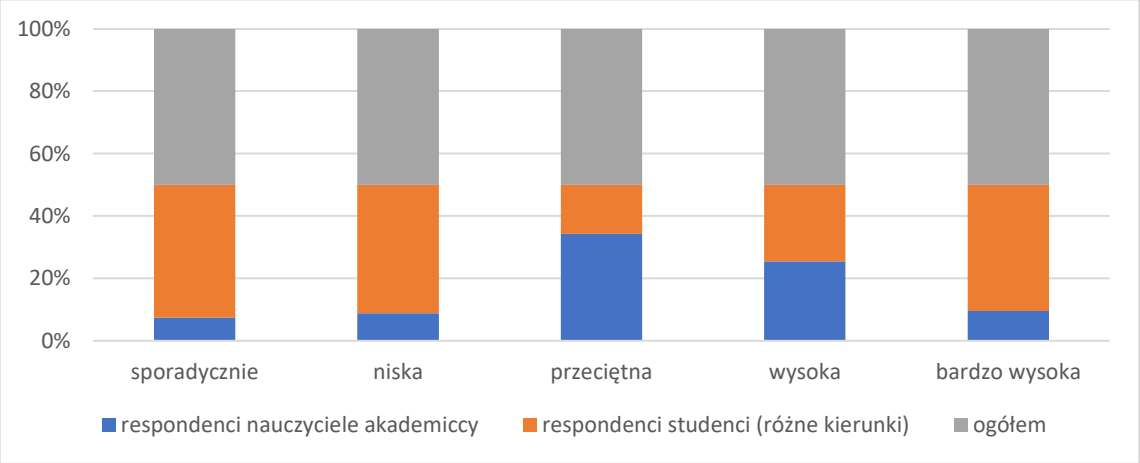
wysoka	30	6%	29	5,8%	59	5,9%
bardzo wysoka	4	0,8%	17	3,4%	21	2,1%
	500	**100%**	**500**	**100%**	**1000**	**100%**

Źródło: opracowanie własne na podstawie badań własnych

W badaniu wzięło udział 500 osób zatrudnionych na stanowisku, nauczycieli akademickich oraz 500 osób studiujących w uczelni wyższej. Z przeprowadzonej analizy wynika, że nauczyciele akademiccy jak i studenci ocenili przestarzałe oprogramowania w uczelni wyższej w stopniu przeciętnym i niskim. Wskazuje na to 412 respondentów, co w udziale procentowym wynosi 82,4% dla nauczycieli akademickich i 196 respondentów, co w udziale procentowym dla studentów wynosi 39,2%.

Analizując udzielone odpowiedzi w opinii 4 respondentów, co w udziale procentowym wynosi 0,8% dla nauczycieli akademickich i 17 respondentów, co w udziale procentowym daje 3,4% dla studentów świadczy, że pojawienie się przestarzałego oprogramowania stanowi bardzo duże zagrożenie dla systemu informacyjnego uczelni wyższej. Wykres 3.129. przedstawia odpowiedzi respondentów grupy nauczyciele akademiccy i grupy studenci (różne kierunki) na temat przestarzałego oprogramowania w uczelni wyższej.

Wykres 3.129. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy studenci (różne kierunki) na temat stopnia zagrożenia systemu uczelni wyższej przez przestarzałe oprogramowania



Źródło: opracowanie własne na podstawie badań własnych

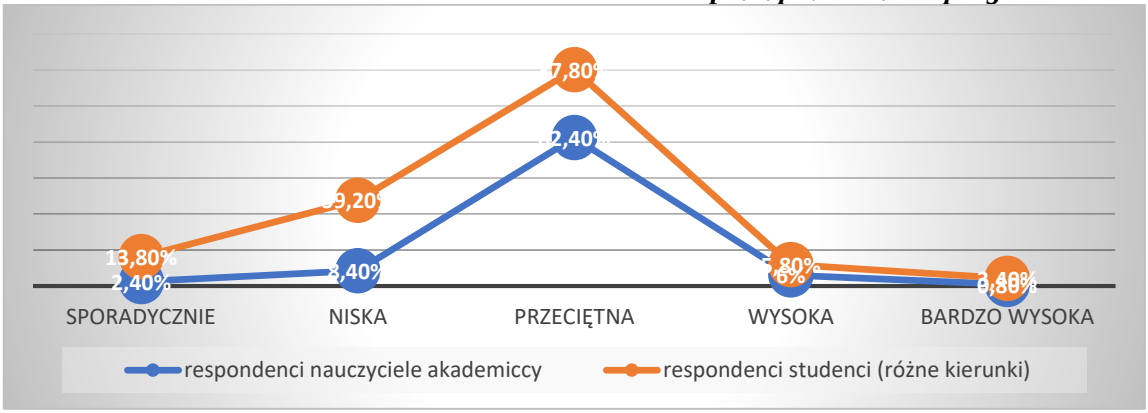
O stopniu zależności świadczy współczynnik korelacji liniowej Pearsona na poziomie 0,62 i współczynnik determinacji liniowej, który wskazuje procent wyjaśnionej

liniowo zmienności równy 38,44%. Wykres 3.130. pokazuje zależność między respondentami grupy nauczyciele akademiccy i grupy studenci (różne kierunki) pod względem stopnia zagrożenia systemu uczelni wyższej przez przestarzałe oprogramowania.

$$r_{xy} = \frac{\frac{1}{n}\sum_{i=1}^{n}(x_i-\bar{x})(y_i-\bar{y})}{S_x S_y}=0{,}62$$

$$\mathrm{WD}=r_{xy}^{2} * 100\% = 38{,}44\%$$

Wykres 3.130. Zależność między respondentami grupy nauczyciele akademiccy i grupy studenci (różne kierunki) pod względem stopnia zagrożenia systemu uczelni wyższej przez przestarzałe oprogramowania



Źródło: opracowanie własne na podstawie badań własnych

W związku z faktem, że wartość liczbowa w ocenie relacji jest dodatnia oznacza to, iż wraz ze wzrostem wartości jednej zmiennej rosną wartości także drugiej. Tabela 3.66. Przedstawia odpowiedzi respondentów grupy kadra administracyjna i grupy studenci (różne kierunki) na temat zagrożeń systemu informacyjnego w uczelni wyższej pod względem przestarzałych oprogramowań.

Tabela 3.66. Odpowiedzi respondentów grupy kadra administracyjna i grupy studenci (różne kierunki) na temat przestarzałego oprogramowania

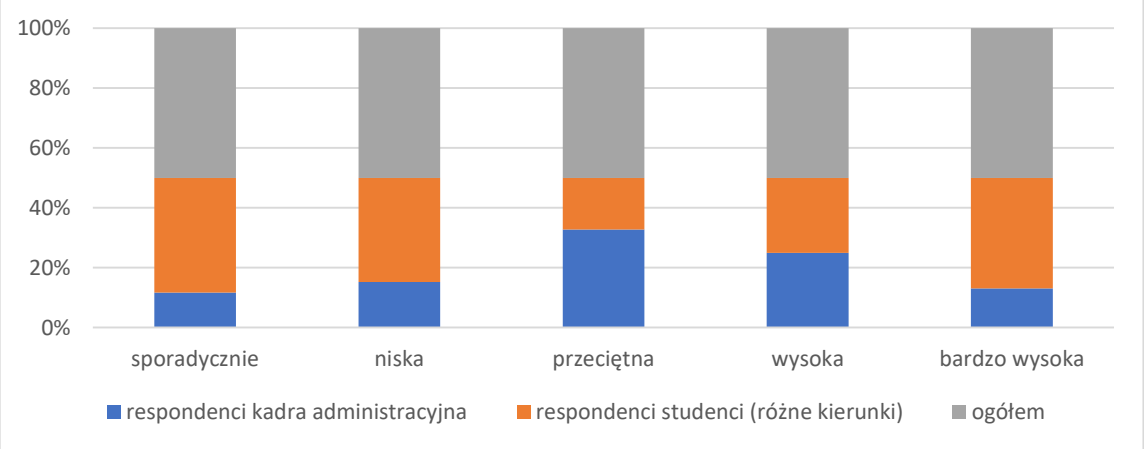
Odpowiedzi badanych osób przestarzałe oprogramowania						
Osoby poddane badaniu	**Respondenci kadra administracyjna**		**Respondenci studenci (różne kierunki)**		**OGÓŁEM**	
Ocena	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***
sporadycznie	21	4,2%	69	13,8%	90	9%
niska	86	17,2%	196	39,2%	282	28,2%
przeciętna	358	71,6%	189	37,8%	547	54,7%
wysoka	29	5,8%	29	5,8%	58	5,8%
bardzo wysoka	6	1,2%	17	3,4%	23	2,3%
	500	**100%**	**500**	**100%**	**1000**	**100%**

Źródło: opracowanie własne na podstawie badań własnych

W badaniu wzięło udział 500 osób zatrudnionych na stanowisku, kadra administracyjna oraz 500 osób studiujących w uczelni wyższej. Z przeprowadzonej analizy wynika, że kadra administracyjna jak i studenci ocenili przestarzałe oprogramowania w uczelni wyższej w stopniu przeciętnym i niskim. Wskazuje na to 358 respondentów, co w udziale procentowym wynosi 71,6% dla kadry administracyjnej i 196 respondentów, co w udziale procentowym dla studentów wynosi 39,2%.

Analizując udzielone odpowiedzi w opinii 6 respondentów, co w udziale procentowym wynosi 1,2% kadry administracyjnej i 17 respondentów, co w udziale procentowym daje 3,4% dla studentów świadczy, że pojawienie się przestarzałego oprogramowania stanowi bardzo duże zagrożenie dla systemu informacyjnego uczelni wyższej. Wykres 3.131. przedstawia odpowiedzi respondentów grupy kadra administracyjna i grupy studenci na temat przestarzałego oprogramowania w uczelni wyższej.

Wykres 3.131. Odpowiedzi respondentów grupy kadra administracyjna i grupy studenci (różne kierunki) na temat stopnia zagrożenia systemu uczelni wyższej przez przestarzałe oprogramowania



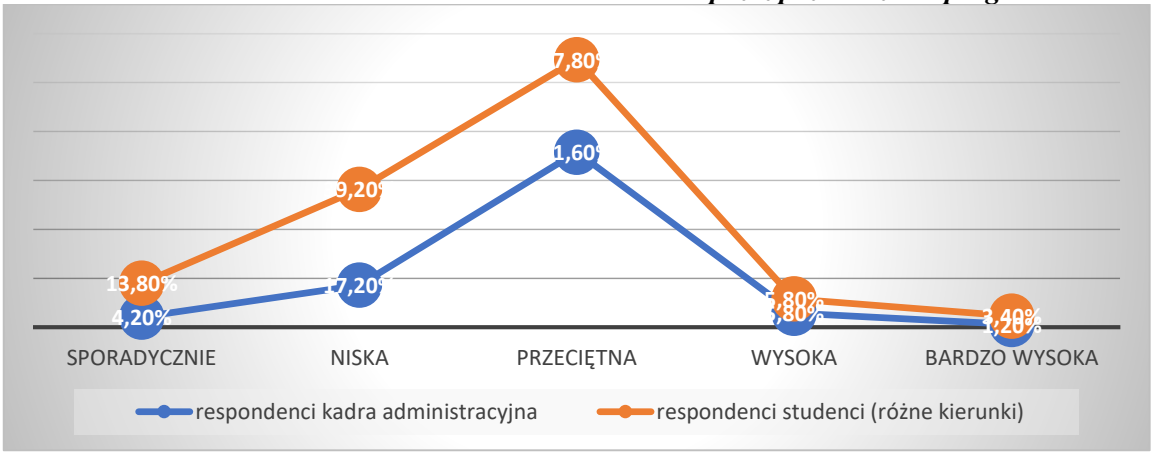
Źródło: opracowanie własne na podstawie badań własnych

O stopniu zależności świadczy współczynnik korelacji liniowej Pearsona na poziomie 0,72 i współczynnik determinacji liniowej, który wskazuje procent wyjaśnionej liniowo zmienności równy 51,84%. Wykres 3.132. pokazuje zależność między respondentami grupy kadra administracyjna i grupy studenci (różne kierunki) pod względem stopnia zagrożenia systemu uczelni wyższej przez przestarzałe oprogramowanie.

$$r_{xy} = \frac{\frac{1}{n}\sum_{i=1}^{n}(x_i-\bar{x})(y_i-\bar{y})}{S_x S_y}=0{,}72$$

$$\mathrm{WD}=r_{xy}^{2} * 100\% = 51{,}84\%$$

Wykres 3.132. Zależność między respondentami grupy kadra administracyjna i grupy studenci (różne kierunki) pod względem stopnia zagrożenia systemu uczelni wyższej przez przestarzałe oprogramowania



Źródło: opracowanie własne na podstawie badań własnych

16. Co Państwa zdaniem jest najczęstszym problemem w sprawach działania systemu w uczelni wyższej?

e) Niewystarczająca ilość komputerów

Rozkład odpowiedzi respondentów grupy nauczyciele akademiccy i grupy kadra administracyjna dotyczący oceny przez użytkowników stopnia problemów związanych z niewystarczającą ilością komputerów w uczelni wyższej prezentuje tabela 3.67.

Tabela 3.67. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy kadra administracyjna na temat niewystarczającej ilości komputerów

Odpowiedzi badanych osób niewystarczająca ilość komputerów						
Osoby poddane badaniu	**Respondenci nauczyciele akademiccy**		**Respondenci kadra administracyjna**		**OGÓŁEM**	
Ocena	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***
sporadycznie	68	13,6%	32	6,4%	100	10%
niska	119	23,8%	369	73,8%	488	48,8%
przeciętna	269	53,8%	89	17,8%	358	35,8%
wysoka	34	6,8%	5	1%	39	3,9%
bardzo wysoka	10	2%	5	1%	15	1,5%
	500	**100%**	**500**	**100%**	**1000**	**100%**

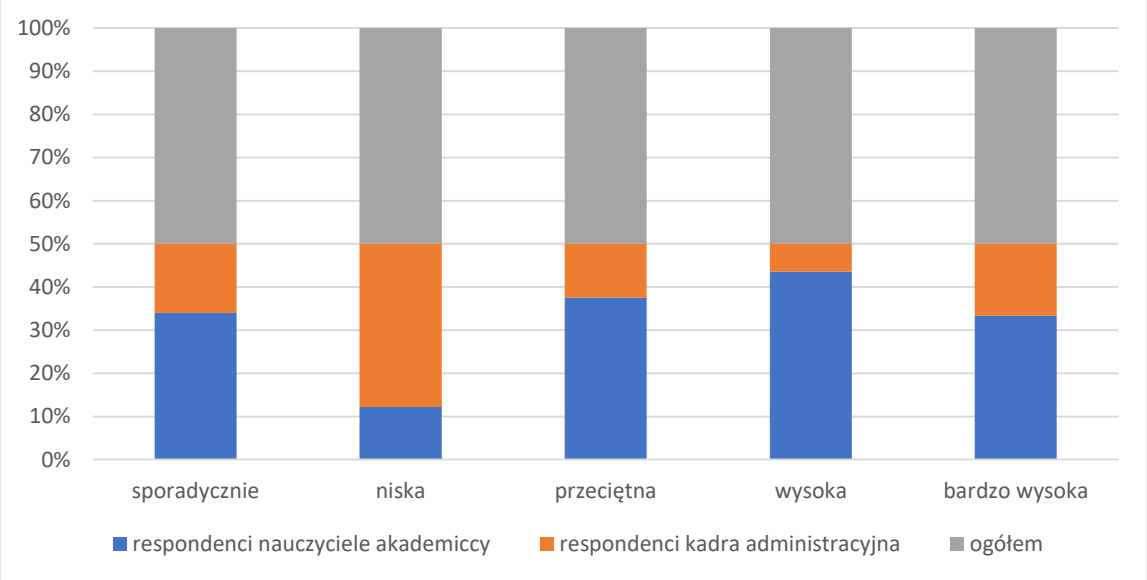
Źródło: opracowanie własne na podstawie badań własnych

W badaniu wzięło udział 500 osób zatrudnionych na stanowisku, nauczycieli akademickich oraz 500 osób zatrudnionych na stanowisku kadry administracyjnej. Z przeprowadzonej analizy wynika, że nauczyciele akademiccy jak i kadra administracyjna oce-

nili niewystarczającą ilość komputerów w uczelni wyższej w stopniu przeciętnym i niskim. Wskazuje na to 269 respondentów, co w udziale procentowym wynosi 53,8% dla nauczycieli akademickich i 369 respondentów, co w udziale procentowym dla kadry administracyjnej wynosi 73,8%.

Analizując udzielone odpowiedzi w opinii 10 respondentów, co w udziale procentowym wynosi 2% dla nauczycieli akademickich i 5 respondentów, co w udziale procentowym daje 1% dla kadry administracyjnej świadczy, że pojawienie się niewystarczającej ilości komputerów stanowi bardzo duże zagrożenie dla systemu informacyjnego uczelni wyższej. Wykres 3.133. przedstawia odpowiedzi respondentów grupy nauczyciele akademiccy i grupy kadra administracyjna na temat niewystarczającej ilości komputerów w uczelni wyższej.

Wykres 3.133. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy kadra administracyjna na temat stopnia zagrożenia systemu uczelni wyższej przez niewystarczającą ilość komputerów



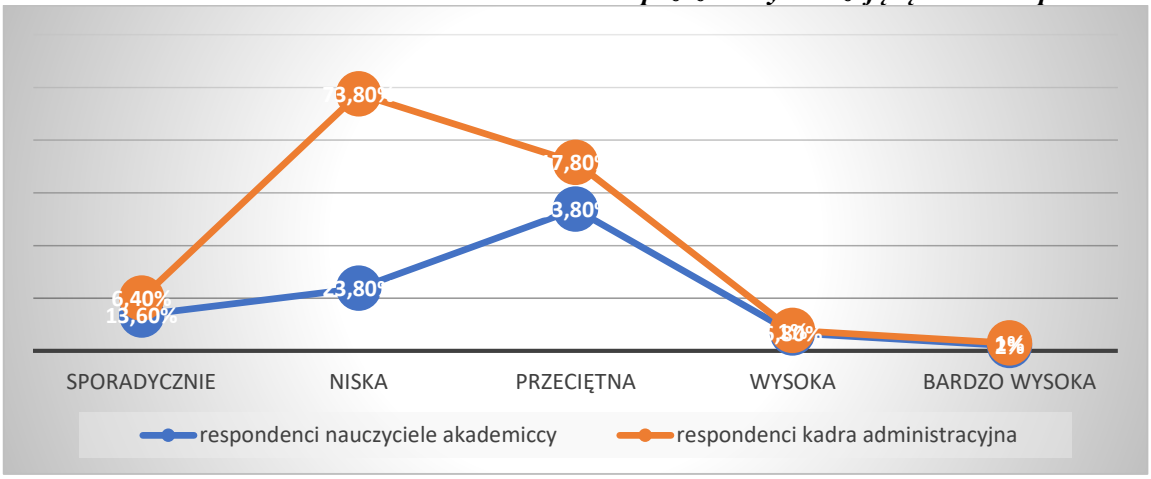
Źródło: opracowanie własne na podstawie badań własnych

O stopniu zależności świadczy współczynnik korelacji liniowej Pearsona na poziomie 0,32 i współczynnik determinacji liniowej, który wskazuje procent wyjaśnionej liniowo zmienności równy 10,24%. Wykres 3.134. pokazuje zależność między respondentami grupy nauczyciele akademiccy i grupy kadra administracyjna pod względem stopnia zagrożenia systemu uczelni wyższej przez niewystarczającą ilość komputerów.

$$r_{xy} = \frac{\frac{1}{n}\sum_{i=1}^{n}(x_i-\bar{x})(y_i-\bar{y})}{S_x S_y}=0{,}32$$

$$\mathrm{WD}=r_{xy}^{2} * 100\% = 10{,}24\%$$

Wykres 3.134. Zależność między respondentami grupy nauczyciele akademiccy i grupy kadra administracyjna pod względem stopnia zagrożenia systemu uczelni wyższej przez niewystarczającą ilość komputerów



Źródło: opracowanie własne na podstawie badań własnych

W związku z faktem, że wartość liczbowa w ocenie relacji jest dodatnia oznacza to, iż wraz ze wzrostem wartości jednej zmiennej rosną wartości także drugiej. Tabela 3.68. przedstawia odpowiedzi respondentów grupy nauczyciele akademiccy i grupy studenci (różne kierunki) na temat zagrożeń systemu informacyjnego w uczelni wyższej przez niewystarczającą ilość komputerów.

Tabela 3.68. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy studenci (różne kierunki) na temat niewystarczającej ilości komputerów

Odpowiedzi badanych osób niewystarczająca ilość komputerów						
Osoby poddane badaniu	**Respondenci nauczyciele akademiccy**		**Respondenci studenci (różne kierunki)**		**OGÓŁEM**	
Ocena	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***
sporadycznie	68	13,6%	79	15,8%	147	14,7%
niska	119	23,8%	116	23,2%	235	23,5%
przeciętna	269	53,8%	258	51,6%	527	52,7%
wysoka	34	6,8%	44	8,8%	78	7,8%
bardzo wysoka	10	2%	3	0,6%	13	1,3%
	500	**100%**	**500**	**100%**	**1000**	**100%**

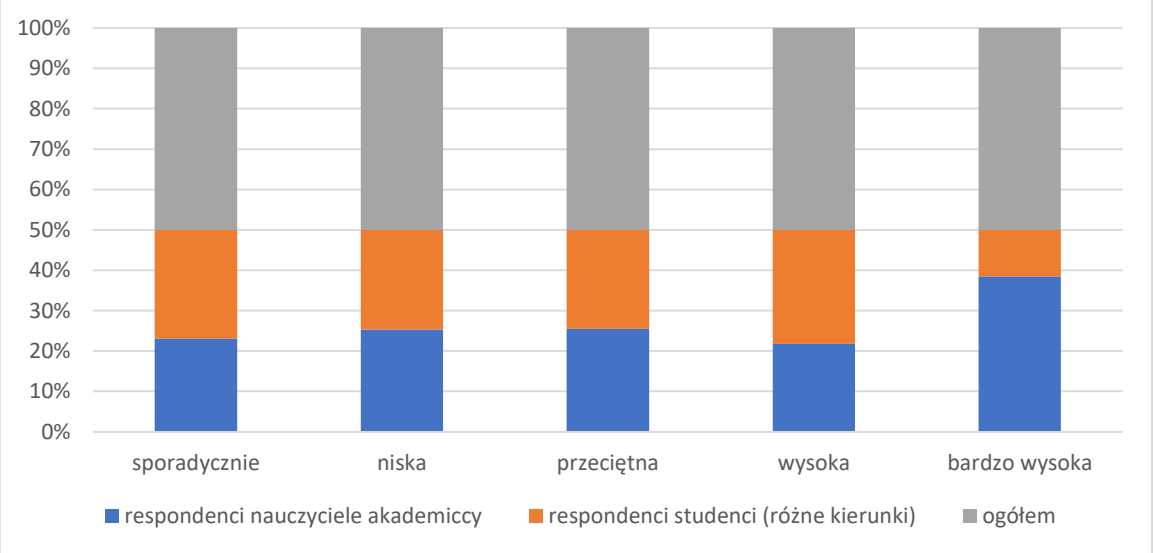
Źródło: opracowanie własne na podstawie badań własnych

W badaniu wzięło udział 500 osób zatrudnionych na stanowisku, nauczycieli akademickich oraz 500 osób studiujących w uczelni wyższej. Z przeprowadzonej analizy wynika, że nauczycieli akademiccy jak i studenci ocenili niewystarczającą ilość komputerów w uczelni wyższej w stopniu przeciętnym. Wskazuje na to 269 respondentów, co

w udziale procentowym wynosi 53,8% dla nauczycieli akademickich i 258 respondentów, co w udziale procentowym dla studentów wynosi 51,6%.

Analizując udzielone odpowiedzi w opinii 10 respondentów, co w udziale procentowym wynosi 2% dla nauczycieli akademickich i 3 respondentów, co w udziale procentowym daje 0,6% dla studentów świadczy, że pojawienie się niewystarczającej ilości komputerów stanowi bardzo duże zagrożenie dla systemu informacyjnego uczelni wyższej. Wykres 3.135. przedstawia odpowiedzi respondentów grupy nauczyciele akademiccy i grupy studenci (różne kierunki) na temat niewystarczającej ilości komputerów w uczelni wyższej.

Wykres 3.135. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy studenci (różne kierunki) na temat stopnia zagrożenia systemu uczelni wyższej przez niewystarczającą ilość komputerów



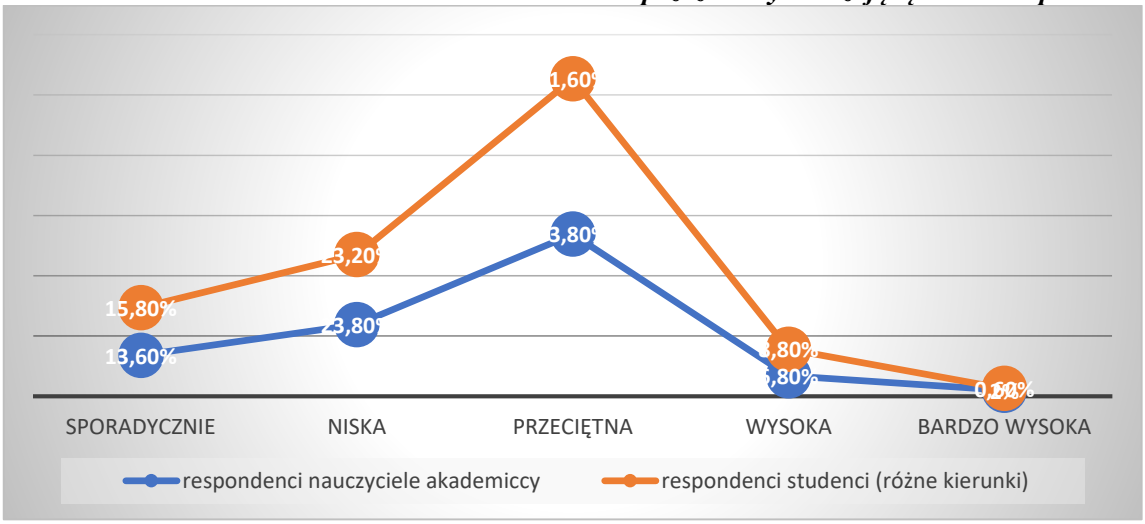
Źródło: opracowanie własne na podstawie badań własnych

O stopniu zależności świadczy współczynnik korelacji liniowej Pearsona na poziomie 0,99 i współczynnik determinacji liniowej, który wskazuje procent wyjaśnionej liniowo zmienności równy 98,01%. Wykres 3.136. pokazuje zależność między respondentami grupy nauczyciele akademiccy i grupy studenci (różne kierunki) pod względem stopnia zagrożenia systemu uczelni wyższej przez niewystarczającą ilość komputerów.

$$r_{xy} = \frac{\frac{1}{n}\sum_{i=1}^{n}(x_i-\bar{x})(y_i-\bar{y})}{S_x S_y}=0{,}99$$

$$\mathrm{WD}=r_{xy}^{2} * 100\% = 98{,}01\%$$

Wykres 3.136. Zależność między respondentami grupy nauczyciele akademiccy i grupy studenci (różne kierunki) pod względem stopnia zagrożenia systemu uczelni wyższej przez niewystarczającą ilość komputerów



Źródło: opracowanie własne na podstawie badań własnych

W związku z faktem, że wartość liczbowa w ocenie relacji jest dodatnia oznacza to, iż wraz ze wzrostem wartości jednej zmiennej rosną wartości także drugiej. Tabela 3.69. przedstawia odpowiedzi respondentów grupy kadra administracyjna i grupy studenci (różne kierunki) na temat zagrożeń systemu informacyjnego w uczelni wyższej przez niewystarczającą ilość komputerów.

Tabela 3.69. Odpowiedzi respondentów grupy kadra administracyjna i grupy studenci (różne kierunki) na temat niewystarczającej ilości komputerów

Odpowiedzi badanych osób niewystarczająca ilość komputerów						
Osoby poddane badaniu	**Respondenci kadra administracyjna**		**Respondenci studenci (różne kierunki)**		**OGÓŁEM**	
Ocena	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***
sporadycznie	32	6,4%	79	15,8%	111	11,1%
niska	369	73,8%	116	23,2%	485	48,5%
przeciętna	89	17,8%	258	51,6%	347	34,7%
wysoka	5	1%	44	8,8%	49	4,9%
bardzo wysoka	5	1%	3	0,6%	8	0,8%
	500	**100%**	**500**	**100%**	**1000**	**100%**

Źródło: opracowanie własne na podstawie badań własnych

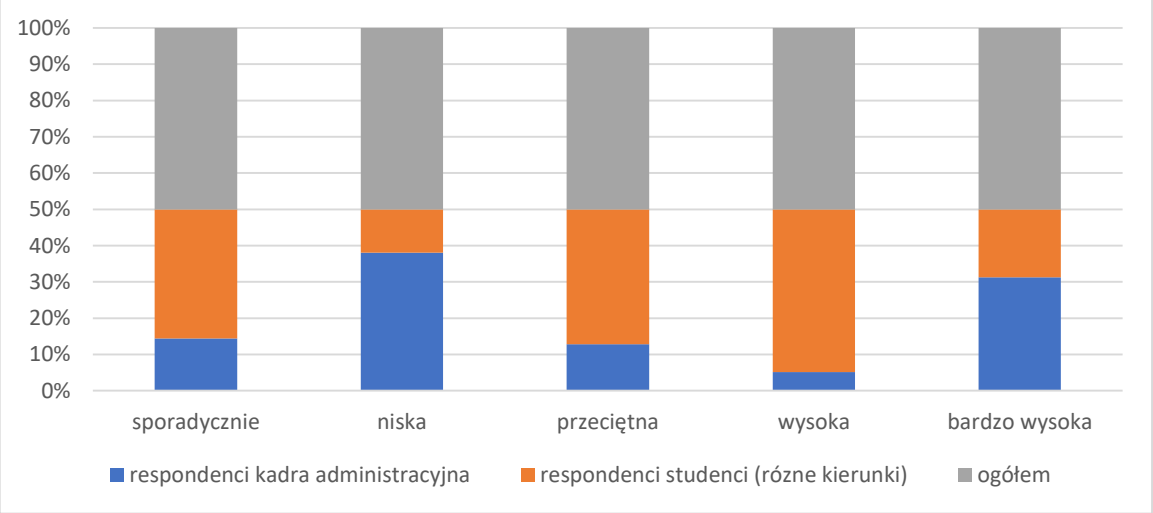
W badaniu wzięło udział 500 osób zatrudnionych na stanowisku, kadra administracyjna oraz 500 osób studentów studiujących na uczelni wyższej. Z przeprowadzonej analizy wynika, że kadra administracyjna jak i studenci ocenili niewystarczającą ilość

komputerów w uczelni wyższej w stopniu niskim i przeciętnym. Wskazuje na to 369 respondentów, co w udziale procentowym wynosi 73,8% dla kadry administracyjnej i 258 respondentów, co w udziale procentowym dla studentów wynosi 51,6%.

Analizując udzielone odpowiedzi w opinii 5 respondentów, co w udziale procentowym wynosi 1% dla kadry administracyjnej i 3 respondentów, co w udziale procentowym daje 0,6% dla studentów świadczy, że pojawienie się niewystarczającej ilości komputerów stanowi bardzo duże zagrożenie dla systemu informacyjnego uczelni wyższej.

Wykres 3.137. przedstawia odpowiedzi respondentów grupy kadra administracyjna i grupy studenci (różne kierunki) na temat niewystarczającej ilości komputerów w uczelni wyższej.

Wykres 3.137. Odpowiedzi respondentów grupy kadra administracyjna i grupy studenci (różne kierunki) na temat stopnia zagrożenia systemu uczelni wyższej przez niewystarczającą ilość komputerów



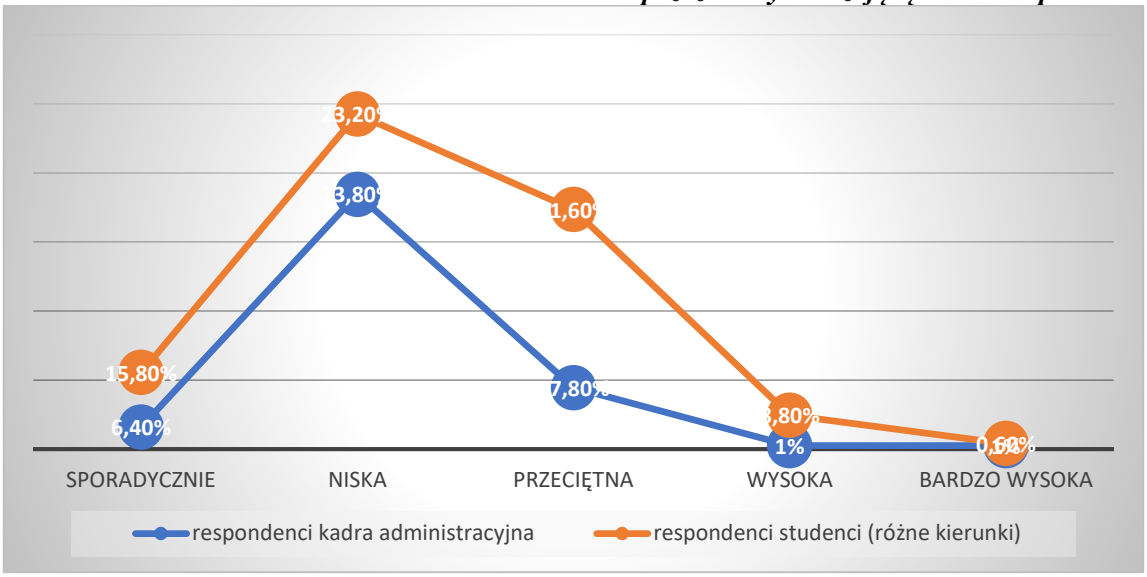
Źródło: opracowanie własne na podstawie badań własnych

O stopniu zależności świadczy współczynnik korelacji liniowej Pearsona na poziomie 0,30 i współczynnik determinacji liniowej, który wskazuje procent wyjaśnionej liniowo zmienności równy 9%. Wykres 3.138. pokazuje zależność między respondentami grupy kadra administracyjna i grupy studenci (różne kierunki) pod względem stopnia zagrożenia systemu uczelni wyższej przez niewystarczającą ilość komputerów.

$$r_{xy} = \frac{\frac{1}{n}\sum_{i=1}^{n}(x_i-\bar{x})(y_i-\bar{y})}{S_x S_y}=0{,}30$$

$$\mathrm{WD}=r_{xy}^{2} * 100\% = 9\%$$

Wykres 3.138. Zależność między respondentami grupy kadra administracyjna i grupy studenci (różne kierunki) pod względem stopnia zagrożenia systemu uczelni wyższej przez niewystarczającą ilość komputerów



Źródło: opracowanie własne na podstawie badań własnych

W związku z faktem, że wartość liczbowa w ocenie relacji jest dodatnia oznacza to, iż wraz ze wzrostem wartości jednej zmiennej rosną wartości także drugiej.

Wnioski

Powyższe działania miały na celu rozwiązanie szczegółowego problemu badawczego zawartego w pytaniu, *Jakie występują zagrożenia bezpieczeństwa systemu informacyjnego w uczelni wyższe?* Przez co także doszło do weryfikacji przyjętej hipotezy, która zakłada, że mnogość użytkowników systemu informacyjnego zmniejsza jego poziom bezpieczeństwa poprzez fragmentaryczne wykorzystanie wszystkich zabezpieczeń i procedur. Bazując na badaniach teoretycznych i empirycznych oraz na własnych doświadczeniach, autorka sprecyzowała następujące wnioski:

- Tradycyjne zagrożenia informacyjne, wskazujące na umyślne działanie idące w kierunku naruszenia ochrony danych, ich ujawnienie osobom nieupoważnionym, ujawnienie danych objętych tajemnicą procedur, ochrony przetwarzania, innych strzeżonych elementów systemu. W celu ich wyeliminowania na powyższe działania należy zwrócić szczególną uwagę i zastosować ścisłą kontrolę użytkowników systemu oraz szerszą analizę ich uprawnień.

- Zagrożenia losowe bezpieczeństwa systemu informacyjnego uczelni wyższej, należy zniwelować poprzez zastosowanie technicznych środków ochronny sprzętu informatycznego. Należy dokonywać systematycznie pełnej archiwizacji, tworząc kopie, które w przypadku wystąpienia potencjalnego zagrożenia nie zakłócą ciągłości pracy szkoły oraz pozwolą odtworzyć wszystkie dane w systemie. Powyższe działania będą korzystne dla ochrony danych systemu.
- Zagrożenia technologiczne, niepożądane modyfikacje w systemie, manipulacja danymi osobowymi w systemie, w tym obszarze skutecznym rozwiązaniem będzie wymiana sprzętu komputerowego na nowy, zawierający pakiet zabezpieczeń bezpośrednio wprowadzony przez producenta. Zastosowanie w posiadanych komputerach nowego oprogramowania, mającego możliwość wyszukania wszelkiego niewłaściwego naruszenia.
- Zagrożeniem, ale i pewnym ograniczeniem dla bezpieczeństwa systemu informacyjnego są niewystarczające umiejętności właściwego korzystania z technologii informacyjnych i komunikacyjnych użytkowników z niego korzystających. Brak elementarnej wiedzy sprzyja cyberprzestępcom, którzy wysyłają wirusy a następnie przejmują hasła dostępu do systemu. Należy inwestować w szerokie i potrzebne szkolenia instruktarzowe, aby podnieść kompetencje i świadomość użytkowników, niwelując deficyt wiedzy wśród użytkowników oraz wskażą, jak korzystać z zabezpieczeń systemu.
- Ograniczeniem skutków dostępu do systemu w wyniku niewylogowania się przed opuszczeniem stanowiska pracy, niezamknięcie pomieszczenia z komputerem. W ramach zwiększenia bezpieczeństwa należy we wszystkich pomieszczeniach w uczelni wyższej zainstalować nawierzchniowe zamki elektroniczne, do otwierania drzwi bez pomocy klucza. Użytkownicy będą mieli możliwość otwarcia drzwi poprzez zeskanowanie odcisku palca oraz poprzez wpisane właściwego kodu bądź włożenie karty pracowniczej, dzięki której system odczyta konkretne przypisanie pracownika do jednostki, działu a tym samym pokoju, w którym pracuje, na co dzień.
- W uczelni wyższej, dostęp do systemu ma bardzo dużo użytkowników, którzy zdecydowanie różnią się od siebie posiadanym wiekiem, kwalifikacjami, doświadczeniem, co znacząco wpływa na zaniżanie progu jego bezpieczeństwa. W związku z powyższym już na etapie koncepcji systemu jego twórcy wprowadzili możliwości różnicowania uprawnień w dostępie do danych i zakresie nałożonych na nich wykonywanych

czynności. Jednakże to zabezpieczenie nie jest wystarczającym gwarantem bezpieczeństwa systemu informacyjnego w uczelni wyższej, przy tak dużej skali użytkowników korzystających z różnych urządzeń i przekaźników przepływu informacji.

4. KONCEPCJA BEZPIECZEŃSTWA SYSTEMU INFORMACYJNEGO

Rozdział czwarty przedstawia koncepcję bezpieczeństwa systemu informacyjnego, nowe kierunki zmian, których celem będzie poprawa bezpieczeństwa systemu na przykładzie publicznej uczelni wyższej. Zmiany te wpisują się w zasadę funkcjonowania i organizacji bezpieczeństwa systemu informacyjnego uczelni wyższej.

Badania, które zostały przeprowadzone w swoich zamierzeniach miały na celu rozwiązanie szczegółowego problemu badawczego zawierającego się w pytaniu:, Jaka ***powinna być koncepcja bezpieczeństwa systemu informacyjnego?*** Aby rozwiązać przedstawiony problem badawczy i zweryfikować hipotezę główną należy stwierdzić, że: ***Obecny system informacyjny w organizacji publicznej na przykładzie publicznej uczelni wyższej nie w pełni chroni informację***. Uszczegółowienie kompetencji użytkowników i przeniesienie na nich odpowiedzialności za utrzymanie stanu bezpieczeństwa informacyjnego. Sytuacja ta będzie miała przełożenie na rozliczenie pracowników z określonych wyników a ten stan rzeczy powinien mieć przełożenie na zachowanie poziomu bezpieczeństwa.

Zastosowanie integracji systemu informacyjnego wszystkich komórek organizacyjnych działających w publicznej uczelni wyższej mający na celu osiągnięcie efektu synergii działań. Kształtowanie dobrych praktyk i porozumienia w zakresie współpracy jednostkowych ogniw operacyjnych występujących w uczelni wyższej. Koniecznym stał się fakt odpowiedzi na przedstawiony problem badawczy i weryfikację sformułowanej hipotezy w związku z powyższym zastosowano następujące metody badawcze, jakimi są:

- *Synteza* – metoda ta miała na celu poznanie istoty zjawiska i scalenia wyników przeprowadzonej analizy w jedną całość;
- *Uogólnienie* – zastosowane zostało przy określeniu poziomu bezpieczeństwa systemu informacyjnego, uwzględniając środowisko wewnętrzne uczelni wyższej. Metoda ta polegała na łączeniu podobnych faktów;
- *Porównanie* – dzięki tej metodzie zostały zidentyfikowane cechy wspólne, podobieństwa jak i różnice poszczególnych badawczych zagadnień. Miało to miejsce w zakresie obiegu informacji w organizacji publicznej, jaką jest uczelnia wyższa oraz bezpieczeństwa tego procesu. Przeprowadzono je podczas porównania skonstruowanego systemu obiegu informacji z rzeczywistym, obecnie funkcjonującym systemem w uczelni wyższej;

- *Wnioskowanie* – metoda ta została wykorzystana we wszystkich rozdziałach dysertacji, zarówno w części poświęconej wnioskom jak i zakończeniu rozpraw;
- *Dedukcja* – miała na celu wskazanie czynników, mających wpływ na bezpieczeństwo systemu informacyjnego w organizacji publicznej, jaką jest uczelnia wyższa oraz uogólnienie wniosków[1];
- *Obserwacja* – metoda ta miała zastosowanie w osobistej i uczestniczącej obserwacji. Została wykorzystana do refleksji nad sytuacją problemową będącą wyjściem do podjętych badań i sformułowania celu ich przeprowadzenia a następnie do analizy i trafnej interpretacji;
- *Metoda sondażu diagnostycznego*[2] – głownie została wykorzystana technika ankiety, jako technika, a jej narzędziem był kwestionariusz ankiety. Pozwoliła na pozyskanie

opinii respondentów odnośnie zapatrywania się na temat zjawiska badanego. Dla uściślenia została wykorzystana metoda wywiadu eksperckiego a jej podstawowym celem było poznanie opinii eksperta w zakresie systemu informacyjnego funkcjonującego w publicznej uczelni wyższej. Opracowana koncepcja bezpieczeństwa systemu informacyjnego w uczelni wyższej nie dotyczy wyłącznie informacji. Zakresem obejmuje system, w którym dochodzi do jej wytworzenia, przetworzenia, przechowywania. Jak również środowisko, w którym ten wspomniany system działa i użytkowników z niego korzystających. Częstym staje się fakt, iż osoby korzystające nie są kontrolowane pod względem posiadanych uprawnień, są lekkomyślne, beztroskie i nieodpowiedzialne.

Duże znaczenie ma także otoczenie formalno-prawne, które wpływa na kształtowanie technologii informacyjnych jak i procesów użytkowania znajdujących się w organizacji użytkowania informacji. Opierając się na spostrzeżeniach autorki należałoby ulepszyć istniejący w uczelni wyższej system informacyjny oraz zainwestować w rozszerzenie już istniejącego systemu informacyjnego zarządzania. Rozszerzenie i wprowadzenie do obecnie już istniejącego systemu bezpieczeństwa obiegu informacji systemów zautomatyzowanych poprawiłoby bezpieczeństwo i skuteczność jej obiegu w wewnętrznym systemie uczelnianym.

[1] W. Pytkowski, Organizacja badań…dz. cyt., s. 117-124.
[2] J. Apanowicz, Metodologia nauk…dz. cyt., s.25-51.

4.1. Zmiany w organizacji systemu informacyjnego

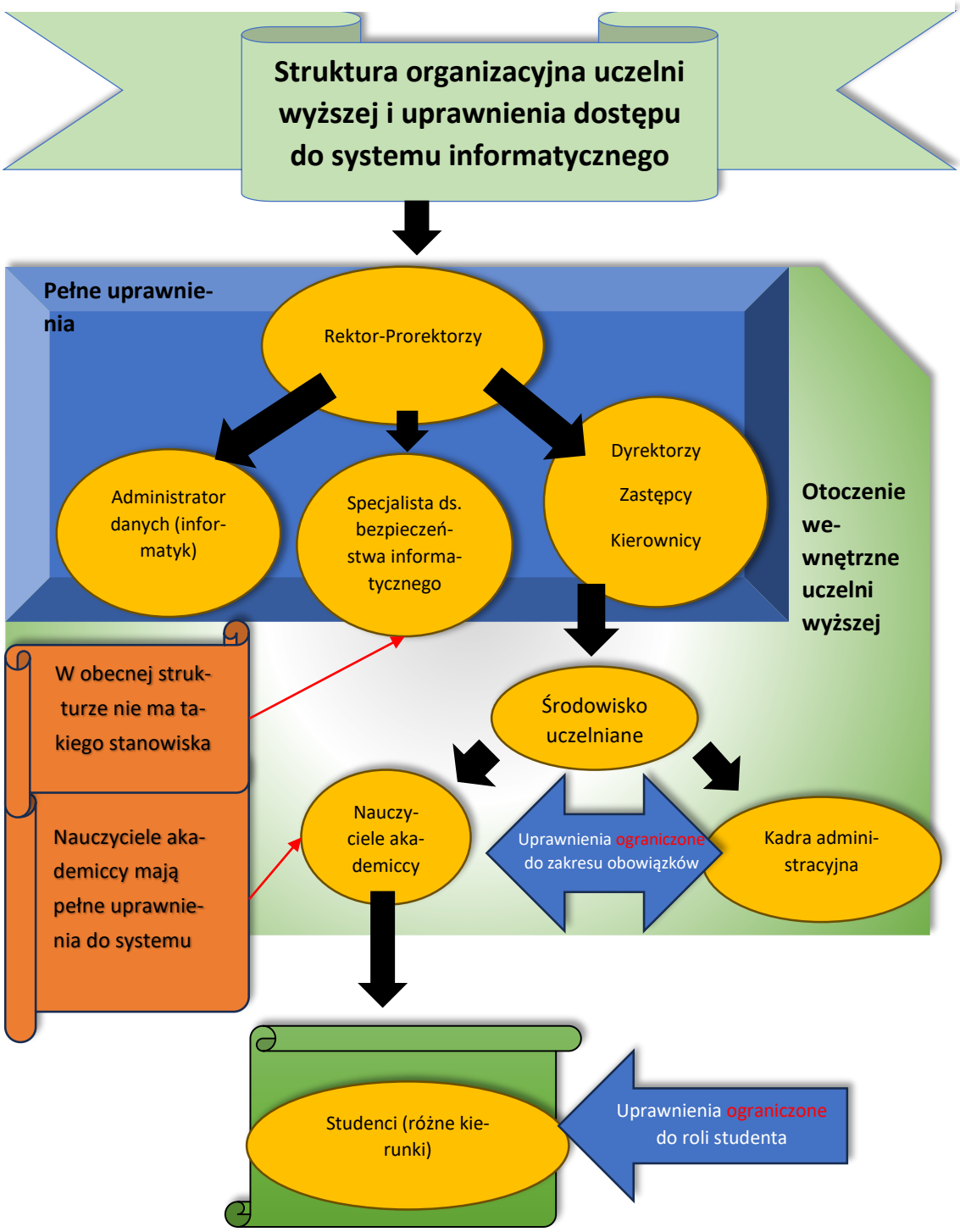
Obszar organizacyjny w uczelni wyższej to nic innego jak ogół jednostek organizacyjnych i podział ich zadań wynikających z wewnętrznych regulaminów. W wyżej wspomnianym obszarze wskazano na konieczność zastosowania integracji systemu informacyjnego wszelkich komórek organizacyjnych prowadzących swoją działalność w uczelni wyższej a celem będzie osiągniecie efektu synergii działań. Koncepcja bezpieczeństwa informacyjnego nie może pominąć w żaden sposób istoty zapewnienia o efektywnej płaszczyźnie porozumienia i budowy dobrych praktyk w zakresie współpracy ogniw operacyjnych występujących w uczelni wyższej.

Założeniem był fakt, iż nadzór i kontrola nad obiegiem informacji w organizacji publicznej powinna być wystarczająca, systematyczna jak i skuteczna. Podstawowymi elementami decydującymi o skuteczności są m.in. częstotliwość, dokładność ich przeprowadzania. Nadzór mający charakter systematyczny, zwiększający bezpieczeństwo informacji będących w obiegu. Bezpieczeństwo systemu informacyjnego to nieodłączny element właściwego funkcjonowania organizacji. W związku z powyższym istotnym elementem w uczelni wyższej jest koncepcja organizacyjna, w której następuje konieczność precyzyjnego określenia hierarchiczności i wytyczenie zadań po to, aby właściwie były realizowane wyznaczone cele i strategia działania uczelni wyższej. Rysunek 4.1. przedstawia strukturę organizacyjną uczelni wyższej i uprawnienia użytkowników do systemu – projekt.

Autorka zaproponowała zmiany dotyczące implementacji pewnych zmian w zasadach użytkowania i organizacji systemu informacyjnego w uczelni wyższej. Przeprowadzone badania dowiodły, iż obecna struktura organizacyjna ogranicza w pełni sprawne funkcjonowanie uczelni wyższej i nie zapewnia pełnego bezpieczeństwa informacyjnego. Powołanie nowej komórki w organizacji odpowiedzialnej za bezpieczeństwo informacyjne spowoduje możliwość realizacji celów i pozwoli na szybsze i skuteczniejsze reagowanie na błędy i incydenty wynikające z niewłaściwego korzystania z kanałów służących do wymiany informacji. Osoba ta będzie mogła dokonywać wnikliwej analizy i kontroli użytkowników systemu. Kolejnym istotnym aspektem, który obejmuje koncepcja to skonkretyzowanie kompetencji poszczególnych użytkowników i nadanie im konkretnych uprawnień do wspomnianego systemu informacyjnego, pozostałe uprawnienia do realizacji zadań w niektórych grupach użytkowników powinny zostać ograniczone. Rysunek

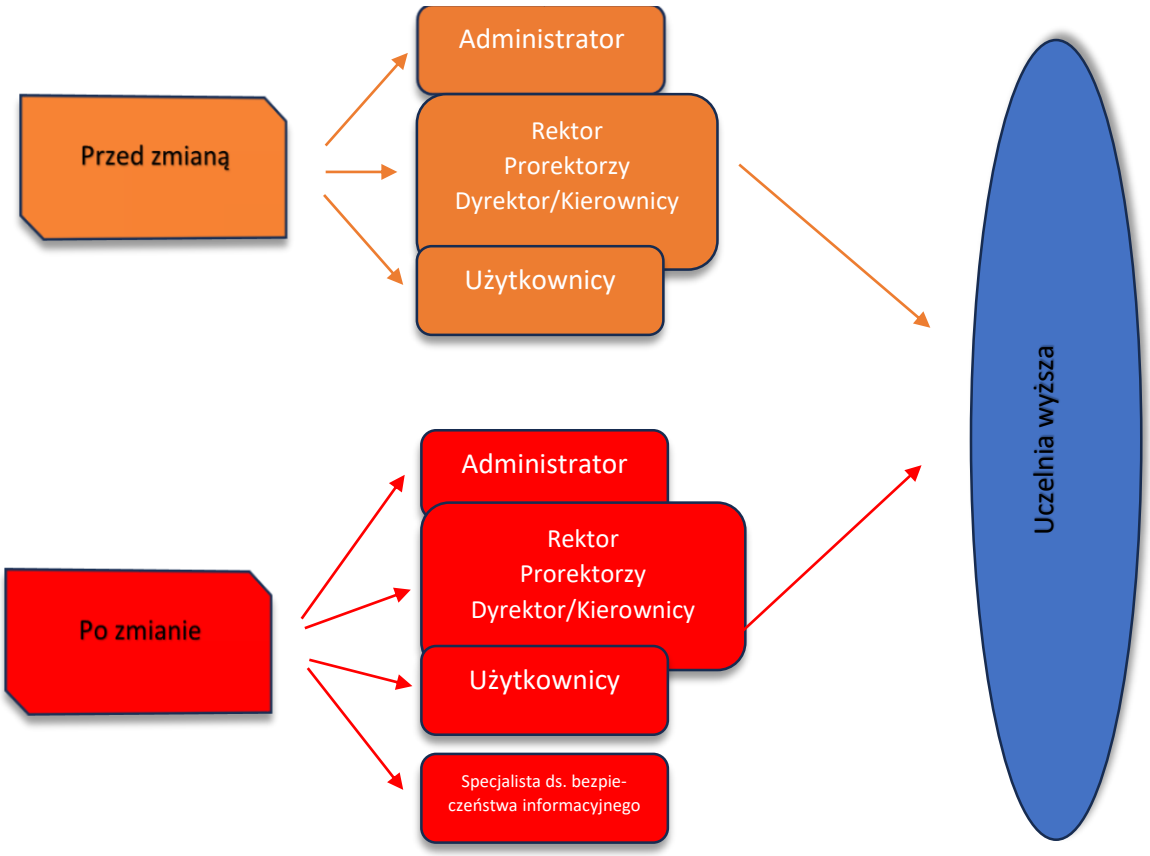
4.2. obrazuje system informacyjny funkcjonujący w uczelni wyższej obecnie funkcjonujący i ze zmianą.

Rysunek 4.1. Struktura organizacyjna uczelni wyższej i uprawnienia użytkowników do systemu – projekt



Źródło: opracowanie własne

Rysunek 4.2. System informacyjny funkcjonujący w uczelni wyższej obecnie funkcjonujący i ze zmianą



Źródło: opracowanie własne

Uprawnienia pełne poza rektorem, prorektorami, kanclerzem i administratorem danych, do systemów wewnętrznych mają również nauczyciele akademiccy i kadra administracja. Przy kadrze administracyjnej jest to w pewnym sensie uzasadnione, ponieważ osoby te w dużej części korzystają z systemów informacyjnych jednakże nie są to wszystkie osoby. Ogromne znaczenie ma tu podział obowiązków, jaki każdy pracownik powinien posiadać od momentu zatrudnienia w uczelni wyższej. Nauczyciele akademiccy posiadają także pełne uprawnienia, co mocno umniejsza bezpieczeństwo systemu informacyjnego w uczelni wyższej. Ta grupa zawodowa nie powinna mieć pełnego dostępu do systemów, ponieważ nie jest to im potrzebne do prowadzenia działań związanych z kształceniem studentów i działalnością naukową. Istnieje także możliwość i niebezpieczeństwo błędnego modyfikowania danych oraz ich ujawnienia poprzez świadome i nieświadome działanie.

Zasady bezpiecznego korzystania z systemu informacyjnego w uczelni wyższej wymagają ciągłego uświadamiania wszystkich użytkowników o konieczności zachowania wszelkich procedur związanych z jego wykorzystaniem. Istotą jest odpowiedzialne podejście pracowników (użytkowników) do procedury utajnienia hasła i w razie konieczności wytypowanie miejsca jego przechowywania w taki sposób, aby osoby trzecie nie miały do niego dostępu.

W badaniach empirycznych została dokonana ocena postępowania użytkowników systemu uczelni wyższej a dotyczy ona działań związanych z hasłami do zasobów sieci. Za pomocą sondażu diagnostycznego w ramach oceny bezpieczeństwa informacji przez respondentów grupy nauczycieli akademickich, kadry administracyjnej, studentów kształcących się na uczelni wyższej, ankietowani mieli możliwość udzielenia odpowiedzi „TAK" lub „ Nie":

2. Czy utrzymujecie Państwo w tajemnicy hasło umożliwiające dostęp do zasobów w sieci?

Rozkład odpowiedzi przez respondentów grupy nauczycieli akademickich i grupy kadra administracyjna odnośnie zachowania w tajemnicy hasła dostępu do sieci prezentuje tabela 4.1.

Tabela 4.1. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy kadra administracyjna na temat utrzymania w tajemnicy hasła dostępu do zasobów w sieci

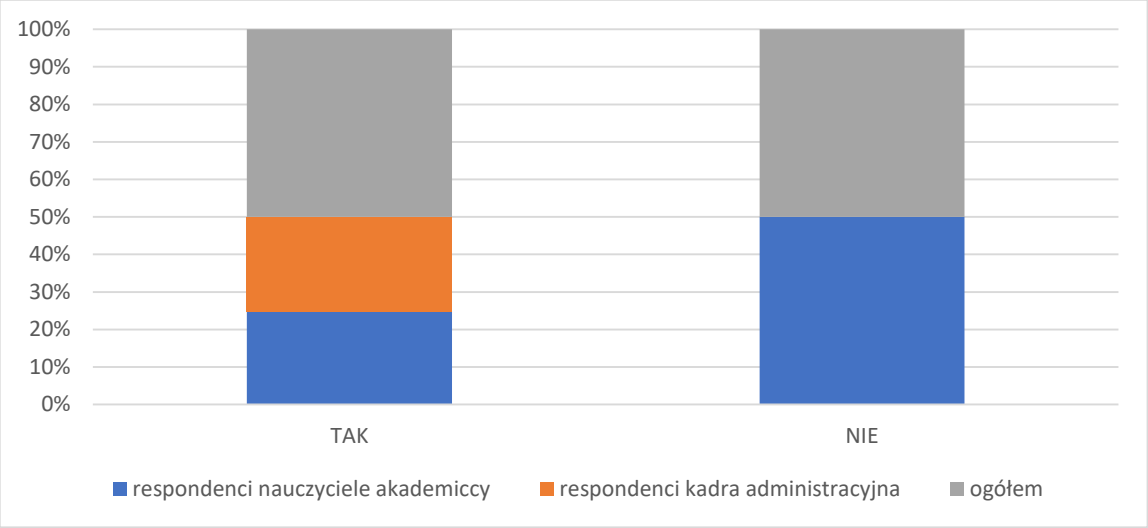
Odpowiedzi badanych osób Tajemnica hasła dostępu do zasobów w sieci							
Osoby poddane badaniu		**Respondenci nauczyciele akademiccy**		**Respondenci kadra administracyjna**		**OGÓŁEM**	
Ocena		***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***
TAK	**KOBIETY**	295	59%	458	91,6%	753	75,3%
	MĘŻCZYŹNI	201	40,2%	42	8,4%	243	24,3%
NIE	**KOBIETY**	3	0,6%	0	0,0%	3	0,3%
	MĘŻCZYŹNI	1	0,2%	0	0,0%	1	0,1%
		500	**100%**	**500**	**100%**	**1000**	**100%**

Źródło: opracowanie własne na podstawie badań własnych

Ogółem na pytanie 3 w kwestionariuszu ankiety dotyczącej utrzymywania w tajemnicy hasła dostępu do zasobów w sieci udzieliło 100% respondentów. Na powyższe pytanie dotyczące utrzymania hasła w tajemnicy pozytywnie wypowiedziało się 295 kobiet wśród grupy nauczycieli akademickich, co w przeliczeniu procentowym daje 59%. W przypadku mężczyzn pozytywną odpowiedź potwierdziło 201 osób co w przeliczeniu procentowym daje 40,2%. Kadra administracyjna wypowiedziała się następująco,

458 kobiet zadeklarowało odpowiedź „TAK” co w przeliczeniu procentowym daje 91,6%, zaś mężczyzn 42, co w przeliczeniu procentowym daję 8,4%. Odpowiedź „NIE” łącznie z obydwu badanych grup zadeklarowało 6 kobiet i 2 mężczyzn.

Wykres 4.1. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy kadra administracyjna na temat utrzymania w tajemnicy hasła dostępu do zasobów sieci



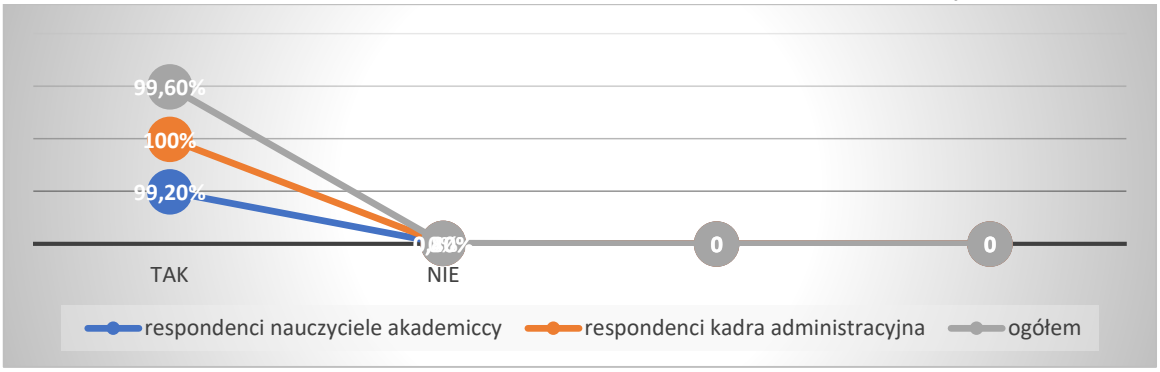
Źródło: opracowanie własne na podstawie badań własnych

Poddane analizie grupy badawcze w zdecydowanej większości potwierdziły, że zachowują w tajemnicy hasła do systemu. Na zależność między zmiennymi wskazuje współczynnik korelacji liniowej Pearsona na poziomie 0,82 i współczynnik determinacji liniowej, procent wyjaśnionej liniowo zmienności równy 67,24 %.

$$r_{xy} = \frac{\frac{1}{n}\sum_{i=1}^{n}(x_i-\bar{x})(y_i-\bar{y})}{S_x S_y}=0{,}82$$

$$\text{WD}=r_{xy}^{2} * 100\% = 67{,}24\%$$

Wykres 4.2. Zależność miedzy respondentami grupy nauczyciele akademiccy i grupy kadra administracyjna pod względem utrzymywania w tajemnicy hasła dostępu do zasobów w sieci



Źródło: opracowanie własne na podstawie badań własnych

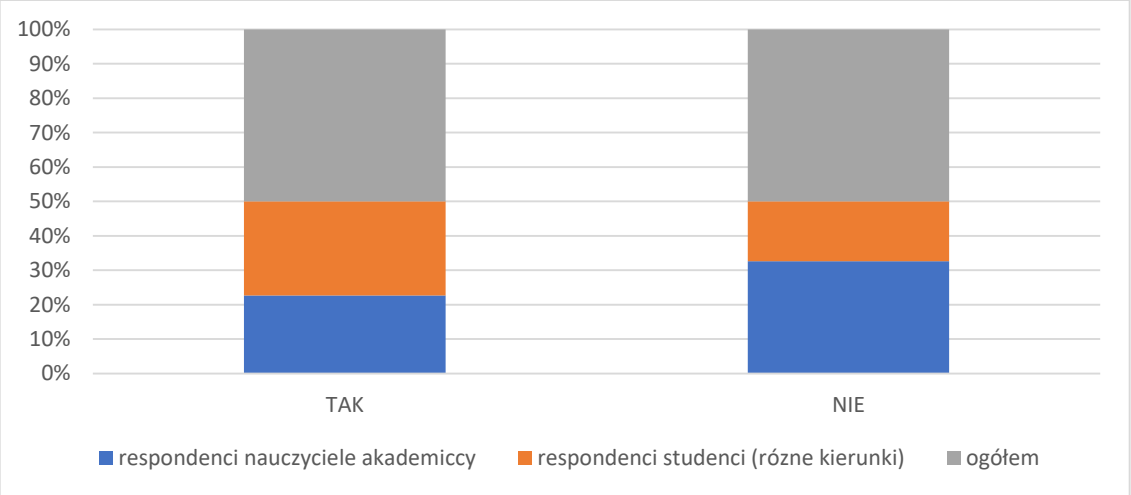
Wraz ze spadkiem wartości jednej z grup respondentów maleją wartości grupy drugiej, co oznacza bardzo silną współzależność dodatnią. Nauczyciele akademiccy wskazali w niewielkim stopniu, że mają odstępstwa od zachowania w tajemnicy swoich haseł, zaś kadra administracyjna zadeklarowała, że takich danych nie udostępnia osobom postronnym. W tabeli 4.2. został zaprezentowany rozkład odpowiedzi respondentów na temat zachowania w tajemnicy hasła dostępu do sieci wśród grupy nauczycieli akademickich i studentów.

Tabela 4.2. Odpowiedzi respondentów grupy nauczyciele akademiccy i studenci na temat utrzymania w tajemnicy hasła dostępu do zasobów w sieci

Odpowiedzi badanych osób Tajemnica hasla dostępu do zasobów w sieci							
Osoby poddane badaniu		**Respondenci nauczyciele akademiccy**		**Respondenci studenci (różne kierunki)**		**OGÓŁEM**	
Ocena		***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***
TAK	**KOBIETY**	295	59%	356	71,2%	651	65,1%
	MĘŻCZYŹNI	201	40,2%	107	21,4%	308	30,8%
NIE	**KOBIETY**	3	0,6%	25	5%	28	2,8%
	MĘŻCZYŹNI	1	0,2%	12	2,4%	13	1,3%
		500	**100%**	**500**	**100%**	**1000**	**100%**

Źródło: opracowanie własne na podstawie badań własnych

Wykres 4.3. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy studenci na temat utrzymywania w tajemnicy hasła dostępu do zasobów w sieci



Źródło: opracowanie własne na podstawie badań własnych

Poddane analizie grupy badawcze w zdecydowanej większości potwierdziły, że zachowują w tajemnicy hasła do systemu. Wśród nauczycieli akademickich jest to 99,6%,

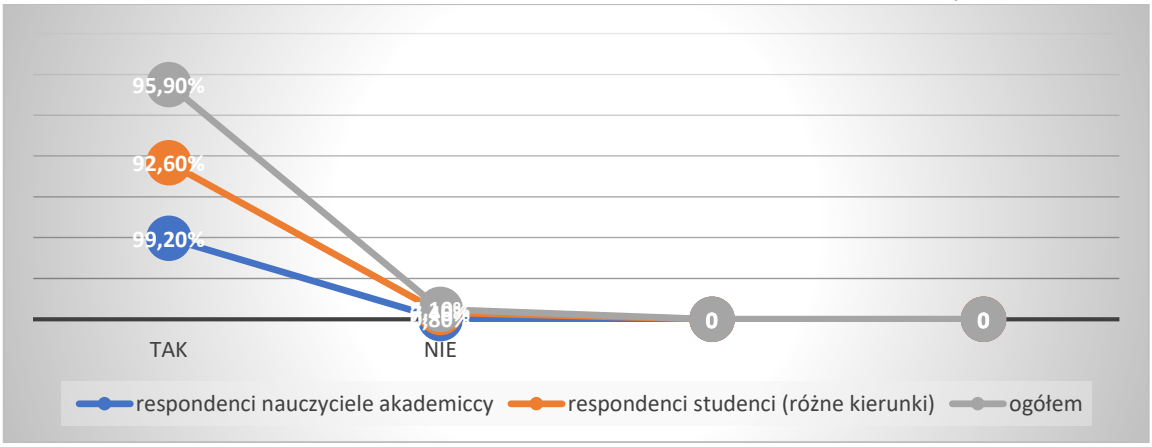
zaś wśród studentów 92,6%. Odpowiedź „TAK" wśród grupy studentów zadeklarowało 356 kobiet i 107 mężczyzn co w przeliczeniu procentowym daje 71,2% i 21,4%. Na postawione pytanie, odpowiedź „Nie" w grupie studentów zadeklarowało 25 kobiet i 12 mężczyzn, co w przeliczeniu daje 5% oraz 2,4%.

Na zależność między zmiennymi wskazuje współczynnik korelacji liniowej Pearsona na poziomie 0,91 i współczynnik determinacji liniowej, procent wyjaśnionej liniowo zmienności równy 82,81%.

$$r_{xy} = \frac{\frac{1}{n}\sum_{i=1}^{n}(x_i-\bar{x})(y_i-\bar{y})}{S_x S_y}=0{,}91$$

$$\text{WD}=r_{xy}^{2} * 100\% = 82{,}81\%$$

Wykres 4.4. Zależności miedzy respondentami grupy nauczyciele akademiccy i grupy studenci różne kierunki pod względem utrzymania w tajemnicy hasła do zasobów w sieci



Źródło: opracowanie własne na podstawie badań własnych

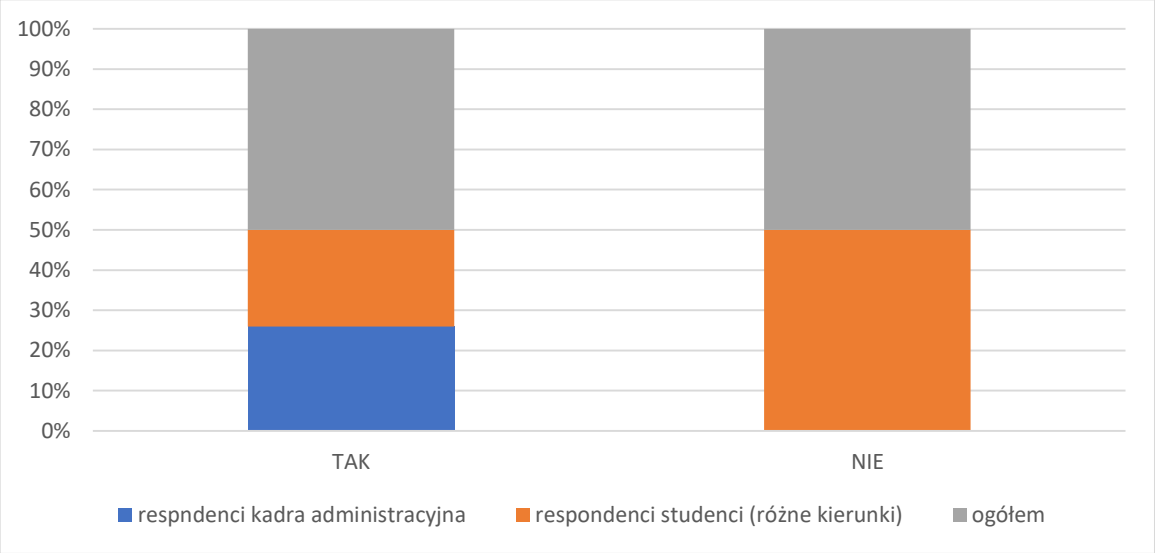
Z badań wynika, że studenci także w dużym stopniu zachowują swoje hasła i nie udostępniają ich osobom trzecim. Tylko 5% kobiet i 2,4 % mężczyzn jest w sprzeczności i udostępnia posiadane hasła osobom do tego nieuprawnionym. Takie zachowanie jest wynikiem dosyć niskiej świadomości studentów na temat pojawiających się zagrożeń. Często studenci nie radzą sobie z wewnętrznymi systemami i ich użytkowaniem oraz obsługą cyfrowych narzędzi w tym elektronicznego systemu wewnętrznego, jakim jest wirtualna uczelnia czy system USOS. Analizując wyniki widać, że jest wysoka korelacja dodatni współczynnika Pearsona. Rozkład odpowiedzi na temat utrzymania w tajemnicy haseł dostępu do sieci wśród grupy kadry administracyjnej i grupy studentów przedstawia tabela 4.3.

Tabela 4.3. Odpowiedzi respondentów grupy kadra administracyjna i grupy studenci (różne kierunki) na temat utrzymania w tajemnicy hasła dostępu do zasobów w sieci

Odpowiedzi badanych osób Tajemnica hasła dostępu do zasobów w sieci							
Osoby poddane badaniu		**Respondenci kadra administracyjna**		**Respondenci studenci (różne kierunki)**		**OGÓŁEM**	
Ocena		***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***
TAK	**KOBIETY**	458	91,6%	356	71,2%	814	81,4%
	MĘŻCZYŹNI	42	8,4%	107	21,4%	149	14,9%
NIE	**KOBIETY**	0	0,0%	25	5%	25	2,5%
	MĘŻCZYŹNI	0	0,0%	12	2,4%	12	1,2%
		500	**100%**	**500**	**100%**	**1000**	**100%**

Źródło: opracowanie własne na podstawie badań własnych

Wykres 4.5. Odpowiedzi respondentów grupy kadra administracyjna i grupy studenci (różne kierunki) na temat utrzymania w tajemnicy hasła dostępu do zasobów w sieci



Źródło: opracowanie własne na podstawie badań własnych

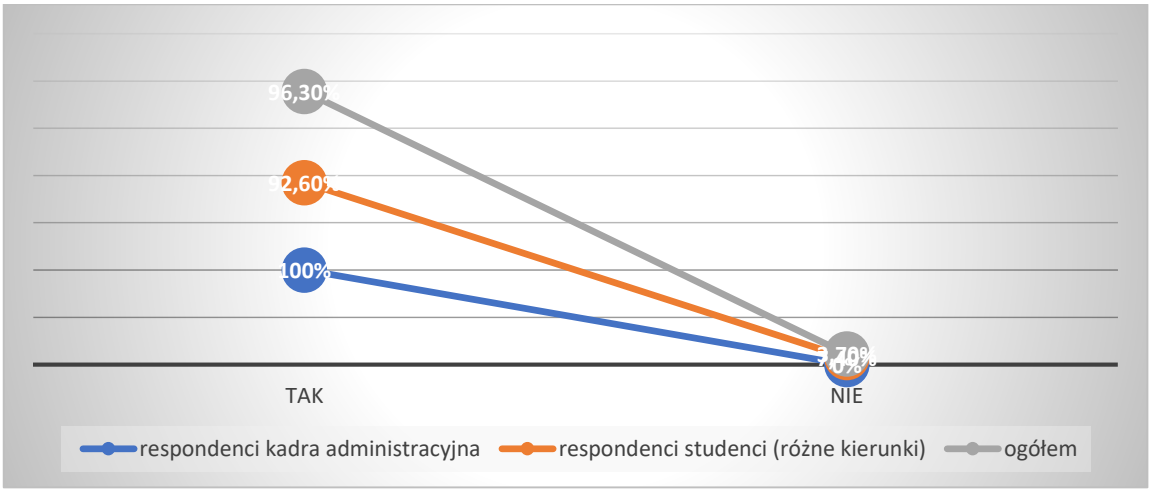
Z analizy danych wynika, że kadra administracyjna bardziej dba o bezpieczeństwo haseł niż studenci. Fakt ten może być spowodowany brakiem świadomości i możliwości wykorzystania takich danych poprzez osoby trzecie jak również może być to spowodowane dużym zaufaniem w znajdującym się środowisku.

Na zależność wskazuje współczynnik korelacji liniowej Pearsona na poziomie 0,98 % i współczynnik determinacji liniowej, który prezentuje procent wyjaśnionej liniowo zmienności 96,4%

$$r_{xy} = \frac{\frac{1}{n}\sum_{i=1}^{n}(x_i-\bar{x})(y_i-\bar{y})}{S_x S_y}=0{,}98$$

$$\text{WD}=r_{xy}^{2} * 100\% = 96{,}4\%$$

Wykres 4.6. Zależność między respondentami grupy kadra administracyjna i grupy studenci (różne kierunki) pod względem utrzymywania w tajemnicy hasła dostępu do zasobów w sieci



Źródło: opracowanie własne na podstawie badań własnych

Należy wnioskować, że odpowiedzi udzielone w kwestionariuszu ankiety przez nauczycieli i pracowników administracji zawierają wymaganą zakresem obowiązków prawidłowość w zachowaniu tajności haseł dostępu do sieci, który wynika z wewnętrznych regulacji wprowadzonych w uczelni wyższej. Z obserwacji jednak wynika, że nie wszystkie osoby w badanych grupach rzeczywiście zachowują tajność haseł dostępu do sieci i częściej robią to kobiety niż mężczyźni. Taka sytuacja wynika z faktu, że to właśnie kobiety posiadają mniejszy zakres wiedzy na temat ryzyka jakie może być następstwem nieprzestrzegania zasad dotyczących bezpieczeństwa. Kobiety są bardziej wylewne, otwarte i szybciej się dzielą pozyskanymi tajemnicami niż mężczyźni.

Nauczyciele akademiccy i kadra administracyjna posiada dużo większe uprawnienia niż studenci w związku z powyższym jest większe ryzyko wśród tej społeczności. To właśnie te dwie grupy dysponują danymi, które mogą wpisywać, modyfikować, przesyłać oraz w razie konieczności anulować. Studenci mają mniejszą świadomość istniejących zagrożeń systemu informacyjnego uczelni wyższej, więc to sprawia, że bez ograniczeń udostępniają dane dotyczące haseł. Jest to także wynikiem młodzieńczego wieku, naiwności i dużego zaufania do osób w ich środowisku. Młodzi ludzie często nie zdają sobie

sprawy z następstw, jakie mogą wynikać z braku odpowiedzialności i przejęcia przez osoby trzecie haseł dostępu do sieci.

W zaproponowanej koncepcji bezpieczeństwa systemu informacyjnego uczelni wyższej, wszyscy pracownicy powinni kierować się kompetencjami, dyscypliną zawodową, pełną świadomością z konsekwencji nie przestrzegania bezpieczeństwa systemu informacyjnego.

Koncepcja obejmuje oprócz pracowników także studentów, wśród których należałoby przeprowadzić szkolenia na spotkaniach z opiekunami roczników odbywających się w częstotliwości nie rzadziej niż raz na semestr. Praktykowane takiego procesu jak podpisywanie oświadczeń, że hasła dostępu przez studentów zostały odebrane i zapoznali się z wymogami obsługi konta nie zapewnia bezpieczeństwa wspomnianego systemu bezpieczeństwa informacyjnego. Wielu użytkowników gubi hasła, zapisuje je w miejscach, które są dostępne dla osób trzecich, zapisują w telefonach czy chociażby logują się a następnie wychodzą z aplikacji bez wylogowania, co w przypadku kradzieży np. telefonu może spowodować łatwy dostęp innej osobie do tego nieuprawnionej.

Ocenie został poddany także fakt nakierowany na pytanie czy użytkownicy systemu w uczelni wyższej stosują zasady bezpieczeństwa w posługiwaniu się swoim loginem i hasłem. Za pomocą sondażu diagnostycznego w ramach oceny poziomu bezpieczeństwa informacji udało się pozyskać odpowiedzi respondentów nauczycieli akademickich, kadry administracyjnej, studentów (różnych roczników). Ankietowani udzielali odpowiedzi z zaproponowanych „ TAK” lub „ NIE”.

3. Czy stosujecie Państwo zasady bezpieczeństwa w posługiwaniu się loginem i hasłem do systemu?

Rozkład odpowiedzi respondentów grupy nauczyciele akademiccy i grupy kadra administracyjna odnośnie zachowania bezpieczeństwa w posługiwaniu się loginem i hasłem do systemu prezentuje tabela 4.4.

Tabela 4.4. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy kadra administracyjna na temat zachowania bezpieczeństwa w posługiwaniu się loginem i hasłem do systemu

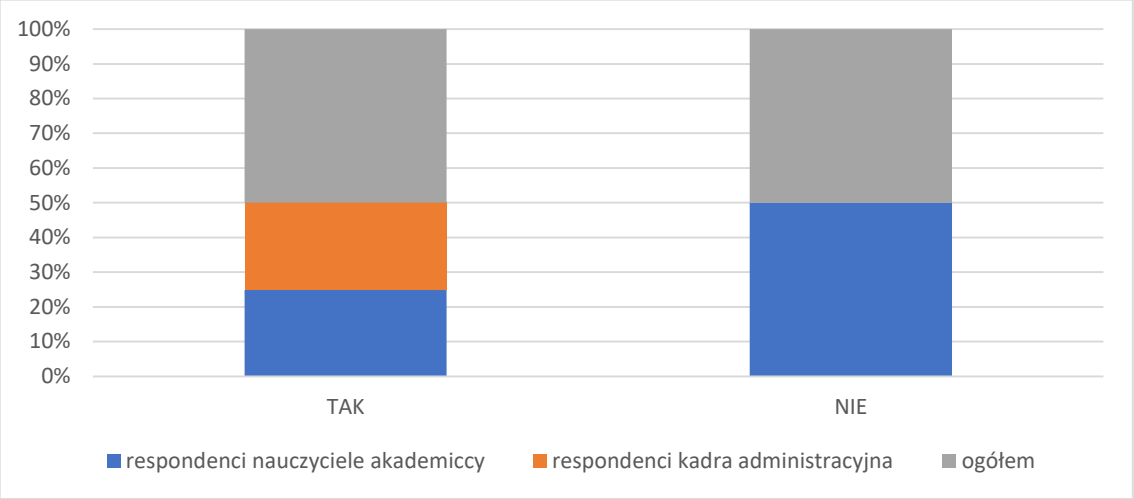
Odpowiedzi badanych osób Zachowanie bezpieczeństwa w posługiwaniu się loginem i hasłem do systemu							
Osoby poddane badaniu		**Respondenci nauczyciele akademiccy**		**Respondenci kadra administracyjna**		**OGÓŁEM**	
Ocena		*liczba wskazań*	*udział procentowy*	*liczba wskazań*	*udział procentowy*	*liczba wskazań*	*udział procentowy*
TAK	**KOBIETY**	295	59%	458	91,6%	753	75,3%
	MĘŻCZYŹNI	201	40,2%	42	8,4%	243	24,3%

NIE	**KOBIETY**	3	0,6%	0	0,0%	3	0,3%
	MĘŻ-CZYŹNI	1	0,2%	0	0,0%	1	0,1%
		500	**100%**	**500**	**100%**	**1000**	**100%**

Źródło: opracowanie własne na podstawie badań własnych

Odpowiedzi na 3 pytanie kwestionariusza ankiety dotyczącego utrzymania bezpieczeństwa w posługiwaniu się loginem i hasłem do systemu udzieliło 100 % respondentów we wszystkich grupach poddanych badaniom.

Wykres 4.7. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy kadra administracyjna na temat zachowania bezpieczeństwa w posługiwaniu się loginem i hasłem do systemu



Źródło: opracowanie własne na podstawie badań własnych

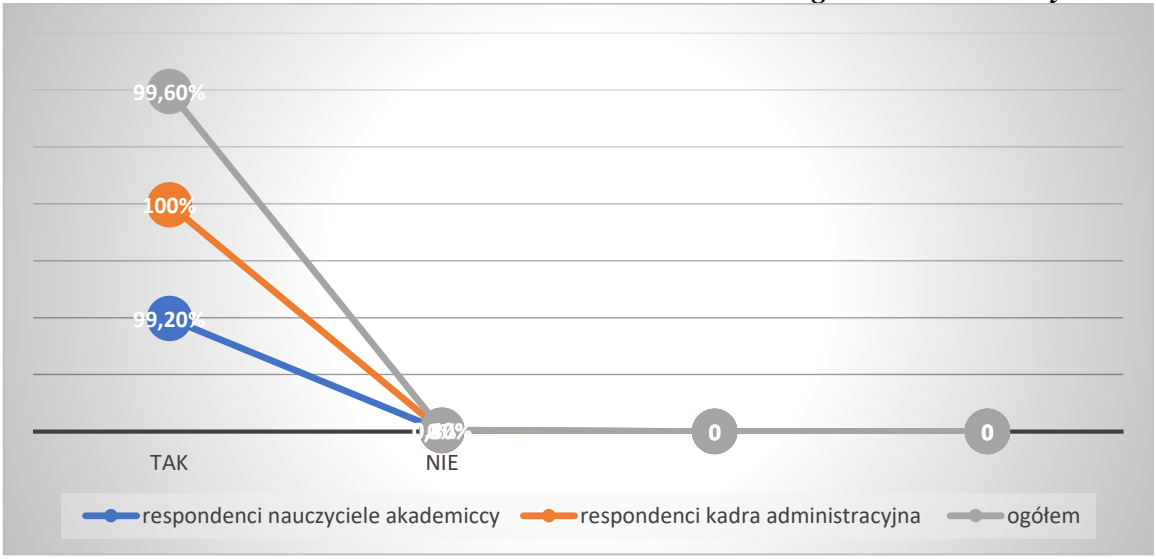
Z przeprowadzonej analizy wynika że nauczyciele akademiccy jak i kadra administracyjna w zdecydowanej większości potwierdziły, iż zasady bezpieczeństwa odnośnie loginów i hasła są wśród nich stosowane. W gronie nauczycieli akademickich jest 99,2% ogółu, zaś wśród kadry administracyjnej to 100% społeczności deklaruje, że zachowuje zasady bezpieczeństwa w przypadku zachowania loginu i hasła do zasobów systemu. Wśród grupy nauczycieli akademickich, 59 % kobiet zadeklarowało zachowanie zasady bezpieczeństwa oraz 40,2% mężczyzn. Sytuacja z grupą kadry administracyjnej była bardzie klarowna, ponieważ to właśnie w tej grupie 91,6% kobiet i 8,4% mężczyzn zadeklarowało, że zachowuje zasady bezpieczeństwa.

Współczynnik korelacji liniowej Pearsona stabilizuje się na poziomie 0,82 i współczynnik determinacji liniowej, który prezentuje procent wyjaśnionej liniowo zmienności jest równy 67,24 %.

$$r_{xy} = \frac{\frac{1}{n}\sum_{i=1}^{n}(x_i-\bar{x})(y_i-\bar{y})}{S_x S_y}=0{,}82$$

$$\text{WD}=r_{xy}^{2} * 100\% = 67{,}24\%$$

Wykres 4.8. Zależność między respondentami grupy nauczyciele akademiccy i grupy kadra administracyjna pod względem zachowania bezpieczeństwa w posługiwaniu się loginem i hasłem do systemu



Źródło: opracowanie własne na podstawie badań własnych

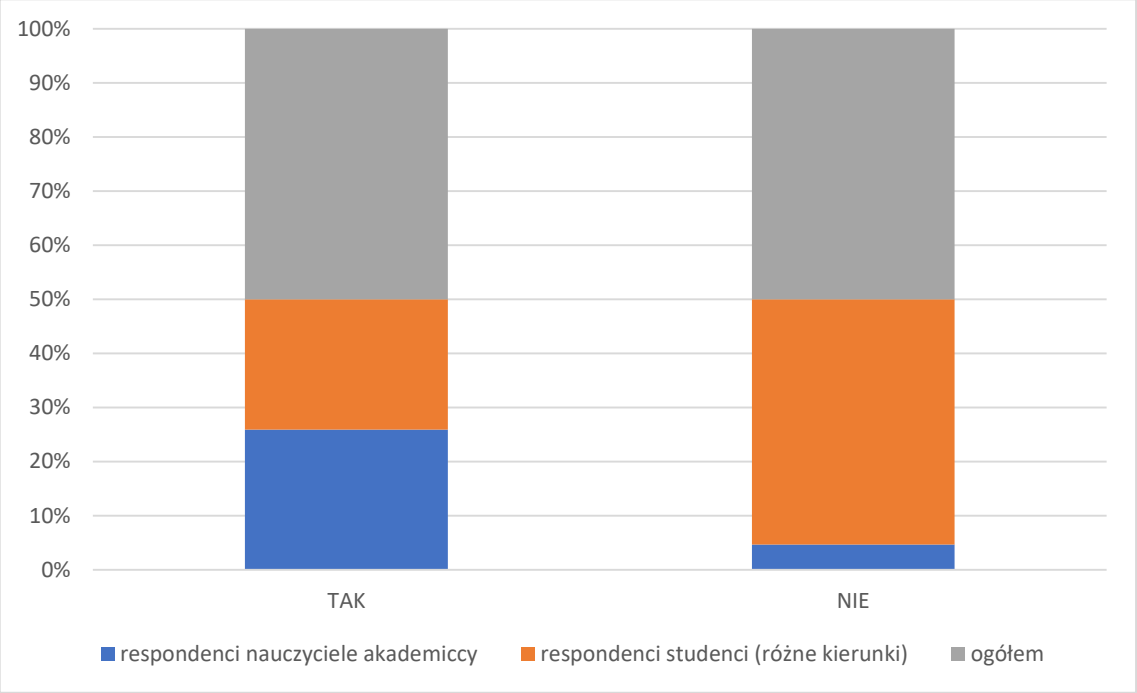
W opinii nauczycieli akademickich i kadry administracyjnej zachodzi współzależność dodatnia a co za tym idzie są stosowane przez te obydwie grupy zasady bezpiecznego posługiwania się loginem i hasłem.

Tabela 4.5. Zaprezentowano rozkład odpowiedzi grupy nauczyciele akademiccy i grupy studenci (różne kierunki) na temat zachowania bezpieczeństwa w posługiwaniu się loginem i hasłem do systemu

Odpowiedzi badanych osób Zachowanie bezpieczeństwa w posługiwaniu się loginem i hasłem do systemu							
Osoby poddane badaniu		**Respondenci nauczyciele akademiccy**		**Respondenci studenci (różne kierunki)**		**OGÓŁEM**	
Ocena		***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***
TAK	**KOBIETY**	295	59%	354	70,8%	649	64,9%
	MĘŻCZYŹNI	201	40,2%	107	21,4%	308	30,8%
NIE	**KOBIETY**	3	0,6%	27	5,4%	30	3%
	MĘŻCZYŹNI	1	0,2%	12	2,4%	13	1,3%
		500	**100%**	**500**	**100%**	**1000**	**100%**

Źródło: opracowanie własne na podstawie badań własnych

Wykres 4.9. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy studenci (różne kierunki) na temat zachowania bezpieczeństwa w posługiwaniu się loginem i hasłem do systemu



Źródło: opracowanie własne na podstawie badań własnych

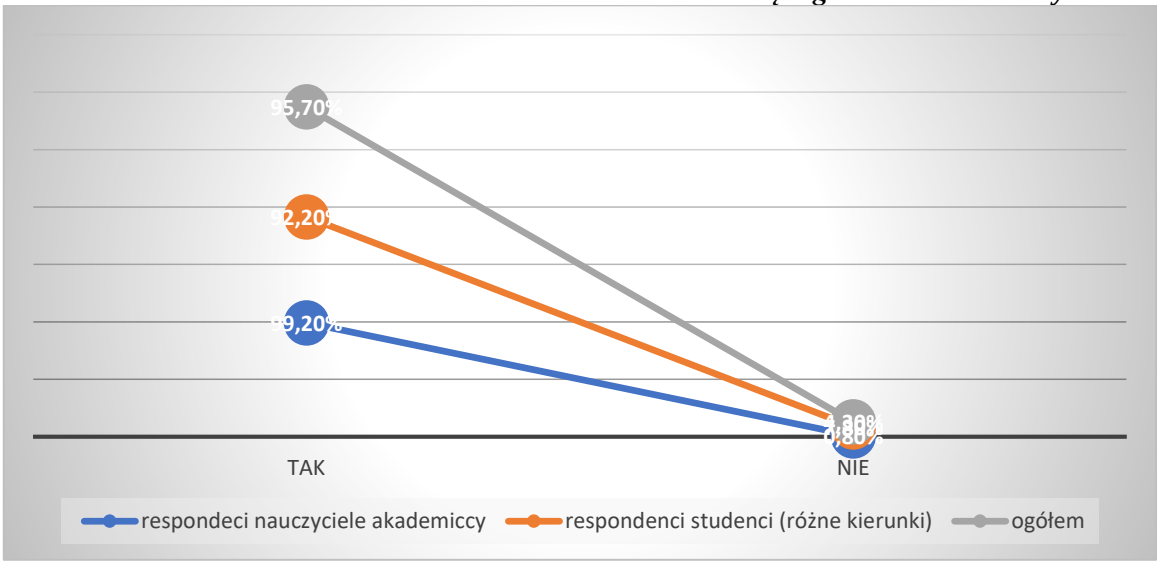
Materiał empiryczny, który został poddany analizie wskazuje, że 461 studentów zadeklarowało, że zachowuje zasady bezpieczeństwa odnośnie wykorzystywania loginu i hasła. W przeliczeniu procentowym wychodzi to 92,2 %. Za zachowaniem bezpieczeństwa optowało 354 kobiet, to daje 70,8% i 107 mężczyzn, czyli 21,4%. Podobnie jak w poprzednim pytaniu to studenci powodują brak zachowania bezpieczeństwa, sytuacja ta jest efektem niskiej świadomości istniejącego zagrożenia, jakie może się pojawić wraz z nieodpowiedzialnym zachowaniem bazującym na dużym zaufaniu wśród osób trzecich.

O zależności świadczy współczynnik korelacji liniowej Pearsona i jest on na poziomie 0,91 a współczynnik determinacji liniowej, wskazuje procent liniowej zmienności na poziomie 82,81%.

$$r_{xy} = \frac{\frac{1}{n}\sum_{i=1}^{n}(x_i-\bar{x})(y_i-\bar{y})}{S_x S_y}=0{,}91$$

$$\mathrm{WD}=r_{xy}^{2} * 100\% = 82{,}81\%$$

Wykres 4.10. Zależność miedzy respondentami grupy nauczyciele akademiccy i grupy studenci (różne kierunki) pod względem zachowania bezpieczeństwa w posługiwaniu się loginem i hasłem do systemu



Źródło: opracowanie własne na podstawie badań własnych

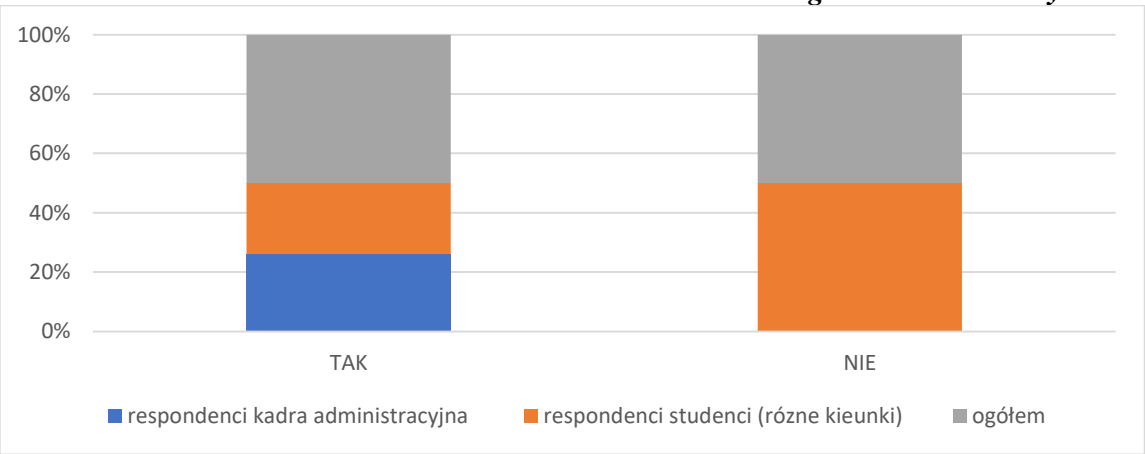
Rozkład odpowiedzi na temat zachowania bezpieczeństwa w posługiwaniu się loginem i hasłem do systemu wśród grupy respondentów kadry administracyjnej i grupy studentów zaprezentowana została w tabeli 4.6.

Tabela 4.6. Odpowiedzi respondentów grupy kadra administracyjna i grupy studenci (różne kierunki) na temat zachowania bezpieczeństwa w posługiwaniu się loginem i hasłem do systemu

Odpowiedzi badanych osób Zachowanie bezpieczeństwa w posługiwaniu się loginem i hasłem do systemu							
Osoby poddane badaniu		**Respondenci kadra administracyjna**		**Respondenci studenci (różne kierunki)**		**OGÓŁEM**	
Ocena		***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***
TAK	**KOBIETY**	458	91,6%	354	70,8%	812	81,2%
	MĘŻCZYŹNI	42	8,4%	107	21,4%	149	14,9%
NIE	**KOBIETY**	0	0,0%	27	5,4%	27	2,7%
	MĘŻCZYŹNI	0	0,0%	12	2,4%	12	1,2%
		500	**100%**	**500**	**100%**	**1000**	**100%**

Źródło: opracowanie własne na podstawie badań własnych

Wykres 4.11. Odpowiedzi respondentów grupy kadra administracyjna i grupy studenci (różne kierunki) na temat zachowania bezpieczeństwa w posługiwaniu się loginem i hasłem do systemu



Źródło: opracowanie własne na podstawie badań własnych

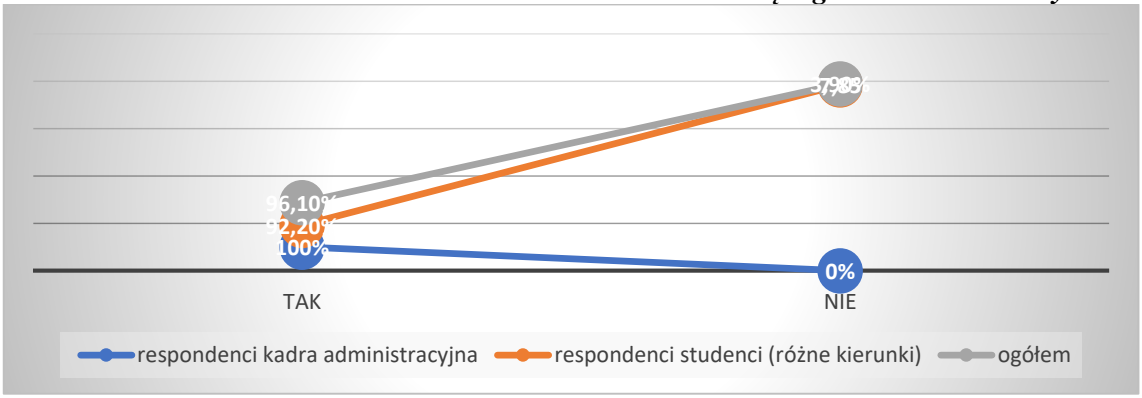
Analizując dane empiryczne można zauważyć, że kadra administracyjna twierdzi, w 100% że zachowuje bezpieczeństwo w posługiwaniu się loginem i hasłem przeznaczonym do systemu. Studenci zaś deklarują mniejszy procent zachowania bezpieczeństwa w powyższych działaniach, więc 7,8% osób zadeklarowało, że nie zachowuje bezpieczeństwa w posługiwaniu się loginem i hasłem do systemu.

Współczynnik korelacji liniowej Pearsona jest na poziomie 0,98 a współczynnik determinacji liniowej jest równy 96,04%

$$r_{xy} = \frac{\frac{1}{n}\sum_{i=1}^{n}(x_i-\bar{x})(y_i-\bar{y})}{S_x S_y}=0{,}98$$

$$\mathrm{WD}=r_{xy}^{2} * 100\% = 96{,}04\%$$

Wykres 4.12. Zależność między respondentami grupy kadra administracyjna i grupy studenci (różne kierunki) pod względem zachowania bezpieczeństwa w posługiwaniu się loginem i hasłem do systemu



Źródło: opracowanie własne na podstawie badań własnych

Przeprowadzona analiza prowadzi do następujących wniosków i widać, że pozyskane odpowiedzi wszystkich grup respondentów wskazują na zachowanie bezpieczeństwa w posługiwaniu się loginem i hasłem do systemu. Studenci uczciwie wypowiedzieli się odnośnie zasady bezpieczeństwa w posługiwaniu się loginem i hasłem. W toku prowadzonej obserwacji osób tego typu jest znacznie więcej i występują w każdej grupie łącznie z nauczycielami akademickimi i kadrą administracyjną. Kobiety wyraźnie wyróżniają się w łamaniu zachowania bezpieczeństwa systemu. Mimo konieczności częstych zmian haseł składających się z dużych liter, małych liter, znaków, cyfr dochodzi do sytuacji, kiedy i takie kody haseł przestępcy są w stanie w szybkim tempie złamać.

Częsty problem z zachowaniem hasła ma usytuowanie w niedbalstwie, pośpiechu, braku posiadanych kompetencji oraz nieświadomości użytkowników. Nauczyciele akademiccy i studenci logują się z miejsc często przypadkowych. Urządzenia mają włączone zapamiętane hasła, w obawie, że zostanie ono zapomniane przez użytkownika i nie będzie możliwości zalogowania się do systemu. Duża część osób nie ma świadomości, że zapisane hasła mogą być łatwo dostępne dla innych użytkowników sieci. Hasła często są zapisywane w notesach i zostawiane w miejscach, do których jest łatwy dostęp.

Mając na uwadze obecne realia w koncepcji przewiduje się rozszerzenie funkcji systemu o podstawową zasadę uwierzytelniania przez uczelniany system chęci, próby zalogowania się przez użytkownika. Należy zwrócić szczególną uwagę na szkolenia z tematu bezpieczeństwa informacyjnego w uczelni wyższej dla wszystkich badanych respondentów, koniecznością było wyeliminowanie nieświadomości społecznej w obszarze, nad którym skupiła się autorka.

Patrząc na wyspecjalizowane grupy cyberprzestępcze w koncepcji dotyczącej bezpieczeństwa systemu informacyjnego należy zaproponować linie papilarne lub skany twarzy zamiast standardowych haseł. Takie hasła stają się być zawodne i niewystarczające, więc z czasem będą one bezzasadne. Technika daje nowe możliwości do rozwoju form zabezpieczenia systemu informacyjnego w uczelni wyższej jednakże należy pamiętać, że wprowadzenie nowych technik cyfrowych musi korelować z wewnętrznym postępem technologicznym i technicznym oraz zasadami wdrożonymi na uczelni wyższej.

Na obecną chwilę jest to koncepcja, jaka może mieć zastosowanie w przyszłości w związku z tak szybkim rozwojem technologicznym, może być dziedziną rozwojową wymagającą badań. Patrząc z perspektywy czasu należy wzmocnić system informacyjny w uczelni wyższej uwzględniając lepsze zabezpieczenia i odpowiednie wyszkolenie ka-

dry informatycznej zajmującej się tak rozwojową dziedziną, jaką są systemy informacyjne i narzędzia w nich wykorzystywane. Wraz z rozwojem techniki, rozwija się także cyberprzestępczość a to wymaga odpowiednich zabezpieczeń, skutecznych rozwiązań, odpowiednich mechanizmów i narzędzi do ich wykrywania. Respondenci w ramach oceny poziomu bezpieczeństwa informacji mieli możliwość udzielenia jednej z dwóch odpowiedzi „TAK", „NIE".

4. Czy w przypadku utraty hasła lub podejrzenia, że hasło zostało wykradzione i odczytane przez osobę do tego nie nieuprawnioną, informujecie Państwo o tym fakcie administratora systemu informacyjnego?

(w przypadku studentów dyrektora lub opiekuna rocznika powołanego zgodnie z decyzją dyrektora konkretnej jednostki). Rozkład odpowiedzi udzielonych przez respondentów grupy nauczyciele akademiccy i grupy kadra administracyjna zostały przedstawione w tabeli 4.7.

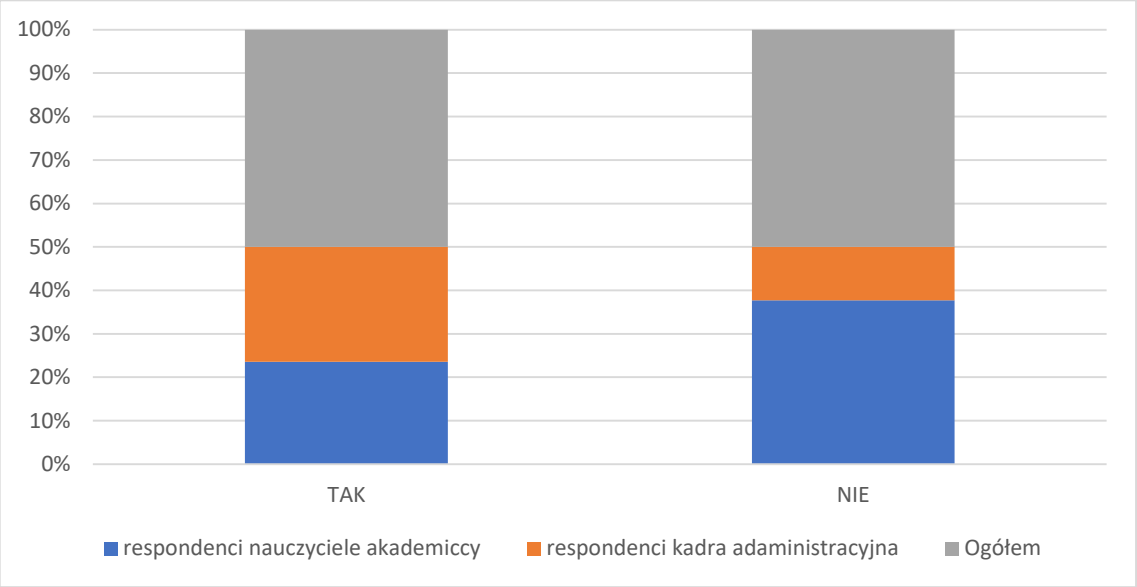
Tabela 4.7. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy kadra administracyjna na temat informowania administratora przez użytkowników uczelnianego systemu w przypadku utraty hasła lub podejrzenia, że zostało wykradzione i odczytane przez osobę nieuprawnioną

Odpowiedzi badanych osób **Informowanie administratora przez użytkowników uczelnianego systemu w przypadku utraty hasła lub podejrzenia, że zostało odczytane/wykorzystane przez osobę nieuprawnioną**							
Osoby poddane badaniu		**Respondenci nauczyciele akademiccy**		**Respondenci kadra administracyjna**		**OGÓŁEM**	
Ocena		***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***
TAK	**KOBIETY**	237	47,4%	440	88%	677	67,7%
	MĘŻCZYŹNI	186	37,2%	35	7%	221	22,1%
NIE	**KOBIETY**	61	12,2%	18	3,6%	79	7,9%
	MĘŻCZYŹNI	16	3,2%	7	1,4%	23	2,3%
		500	**100%**	**500**	**100%**	**1000**	**100%**

Źródło: opracowanie własne na podstawie badań własnych

Podsumowując, odpowiedzi na pytanie 4 kwestionariusza ankiety dotyczącego informowania administratora czy w przypadku studenta informowanie dyrektora lub opiekuna rocznika konkretnej jednostki przez użytkowników uczelnianego systemu w sytuacji utraty hasła czy podejrzeniu, że zostało ono odczytane/wykradzione przez osobę nieuprawnioną na to pytanie 100% respondentów udzieliło odpowiedź we wszystkich badanych grupach.

Wykres 4.13. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy kadra administracyjna na temat informowania administratora przez użytkowników uczelnianego sytemu w przypadku utraty hasła lub podejrzenia, że zostało wykradzione i odczytane przez osobę nieuprawnioną



Źródło: Opracowanie własne na podstawie badań własnych

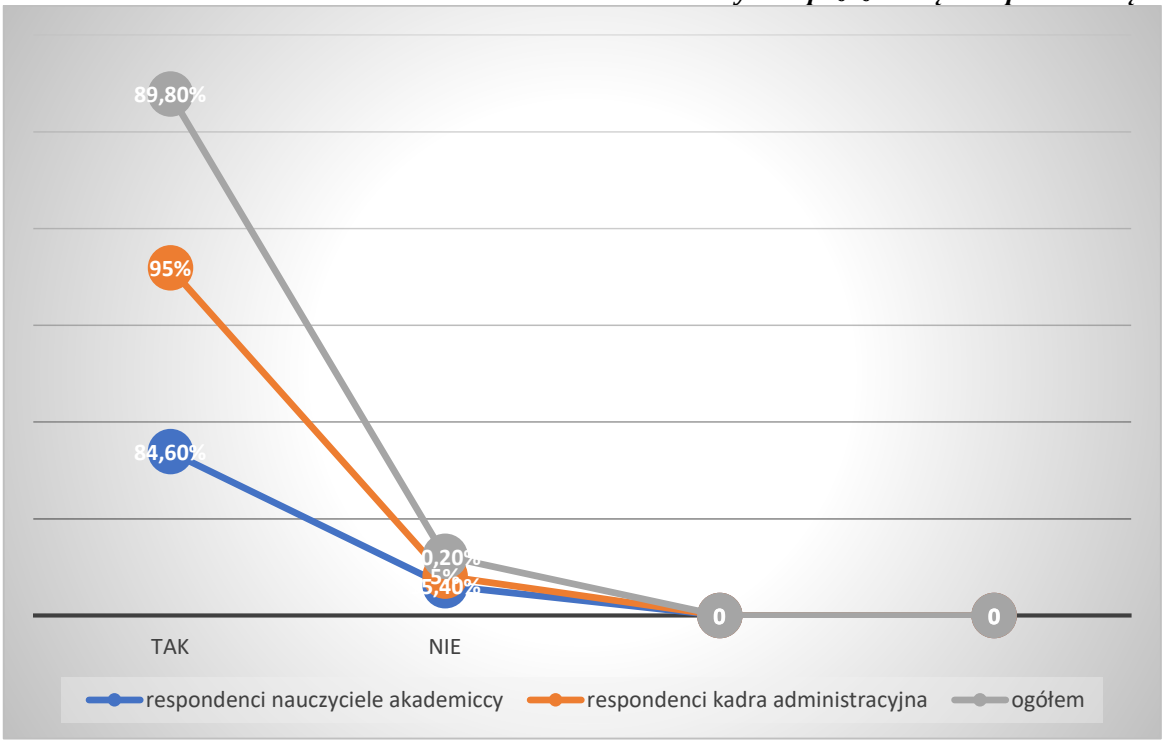
Z analizy danych wynika, że o informowaniu administratora uczelnianego systemu w przypadku utraty hasła lub podejrzenia, że zostało odczytane/wykradzione przez osobę nieuprawnioną w grupie respondentów nauczycieli akademickich potwierdziło dokonanie zgłoszenia 84,6% osób, w tym 47,4% kobiet i 37,2% mężczyzn. W przypadku kadry administracyjnej wyniki kształtują się następująco, łączna ilość to 95%,. Odpowiedź tą zadeklarowało 88% kobiet i 7% mężczyzn. W tych grupach znalazły się także osoby, które nie zgłaszają takiej sytuacji i w przypadku grupy nauczycieli akademickich jest to 15,4% a w przypadku kadry administracyjnej ta liczba wynosi 5%.

Na zależność wskazuje współczynnik korelacji liniowej Pearsona, który jest na poziomie 0,76 i współczynnik determinacji liniowej, przedstawia procent wyjaśnionej ilościowo zmienności i jest równy 57,76%.

$$r_{xy} = \frac{\frac{1}{n}\sum_{i=1}^{n}(x_i-\bar{x})(y_i-\bar{y})}{S_x S_y}=0{,}76$$

$$\mathrm{WD}=r_{xy}^{2} * 100\% = 57{,}76\%$$

Wykres 4.14. Zależności między respondentami grupy nauczyciele akademiccy i grupy kadra administracyjna pod względem informowania administratora przez użytkowników uczelnianego sytemu w przypadku utraty hasła lub podejrzenia, ze zostało wykradzione i odczytane przez osobę nieuprawnioną



Źródło: opracowanie własne na podstawie badań własnych

Uogólniając zauważalna jest współzależność dodatnia pomiędzy tymi badanymi grupami, jakimi są nauczyciele akademiccy i kadra administracyjna. W opinii kadry administracyjnej jest praktykowane zgłaszanie naruszeń związanych z utratą hasła lub jego podejrzeniem o jego odczytanie i wykorzystanie przez osoby trzecie. Większość nauczycieli akademickich także deklaruje tą formę przeciwdziałania w sytuacjach związanymi z utratą hasła lub podejrzeniem go, przez osoby nieuprawnione.

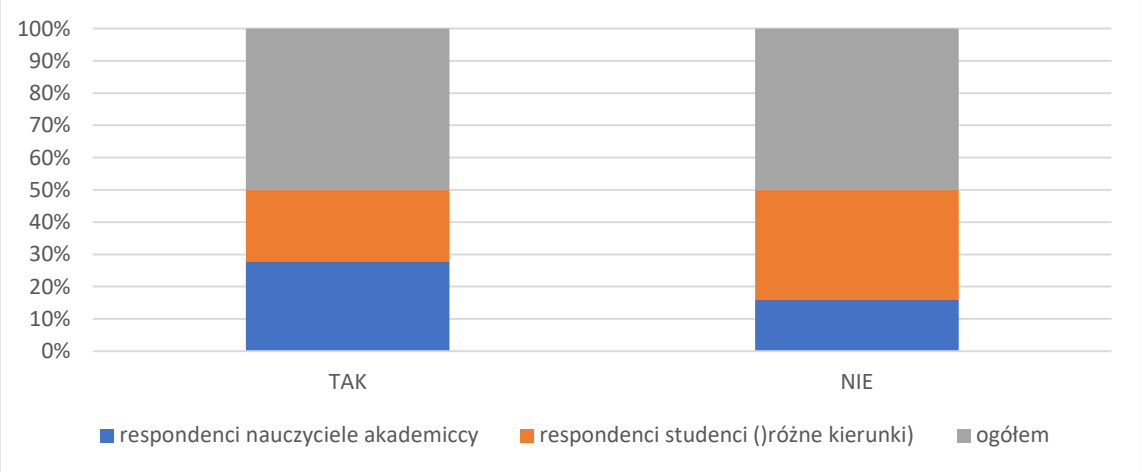
Tabela 4.8. Przedstawia rozkład odpowiedzi dotyczący informowania dyrektora lub opiekuna rocznika konkretnej jednostki przez użytkowników uczelnianego systemu w przypadku utraty hasła lub podejrzenia, że zostało ono odczytane/wykradzione przez osobę nieuprawnioną. Pod uwagę zostały wzięte kolejne grupy takie jak, nauczyciele akademiccy i studenci (różne kierunki).

Tabela 4.8. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy studenci (różne kierunki) na temat informowania administratora przez użytkowników szkolnego systemu w przypadku utraty hasła lub podejrzenia, ze zostało wykradzione i odczytane przez osobę nieuprawnioną

Odpowiedzi badanych osób **Informowanie administratora przez użytkowników uczelnianego systemu w przypadku utraty hasła lub podejrzenia, że zostało odczytane/wykorzystane przez osobę nieuprawnioną**							
Osoby poddane badaniu		**Respondenci nauczyciele akademiccy**		**Respondenci studenci (różne kierunki)**		**OGÓŁEM**	
Ocena		*liczba wskazań*	*udział procentowy*	*liczba wskazań*	*udział procentowy*	*liczba wskazań*	*udział procentowy*
TAK	**KOBIETY**	237	47,4%	251	50,2%	488	48,8%
	MĘŻCZYŹNI	186	37,2%	84	16,8%	270	27%
NIE	**KOBIETY**	61	12,2%	130	26%	191	19,1%
	MĘŻCZYŹNI	16	3,2%	35	7%	51	5,1%
		500	**100%**	**500**	**100%**	**1000**	**100%**

Źródło: opracowanie własne na podstawie badań własnych

Wykres 4.15. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy studenci (różne kierunki) na temat informowania administratora przez użytkowników szkolnego systemu w przypadku utraty hasła lub podejrzenia, ze zostało wykradzione i odczytane przez osobę nieuprawnioną



Źródło: opracowanie własne na podstawie badań własnych

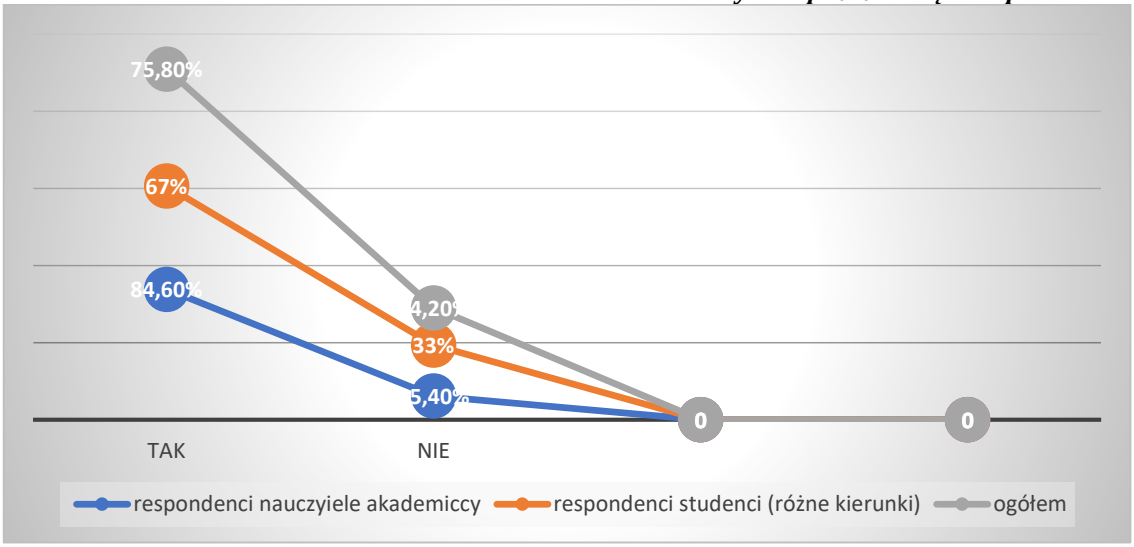
Po dokonaniu analizy wyników badań 84,6% nauczycieli akademickich, w tym kobiet 47,4% i 37,2% mężczyzn deklaruje o poinformowaniu dyrektora/kierownika jednostki lub opiekuna w przypadku utraty hasła lub podejrzenia, że zostało ono odczytane/wykradzione przez osobę nieuprawnioną. Wśród badanych pozostaje 15,4% nauczycieli akademickich w tym 12,2% kobiet i 3,2% mężczyzn, którzy nie informują o powyż-

szym zdarzeniu. Grupa studentów pozytywnie zdeklarowała odpowiedź na zadane pytanie było to 67% respondentów, w tym 50,2% kobiet i 16,8% mężczyzn. Za odpowiedzią „NIE" optowało 24,2% respondentów w grupie studentów, co daje w przeliczeni 19,1% kobiet i 5,1% mężczyzn. O zależności świadczy współczynnik korelacji liniowej Pearsona na poziomie 0,73 i współczynnik determinacji liniowej wskazujący procent wyjaśnionej liniowo zmienności na poziomie 53,29%.

$$r_{xy} = \frac{\frac{1}{n}\sum_{i=1}^{n}(x_i-\bar{x})(y_i-\bar{y})}{S_x S_y}=0{,}73$$

$$\text{WD}=r_{xy}^{2} * 100\% = 53{,}29\%$$

Wykres 4.16. Zależności pomiędzy respondentami grupy nauczyciele akademiccy i grupy studenci (różne kierunki) pod względem informowania administratora przez użytkowników uczelnianego systemu w przypadku utraty hasła lub podejrzenia, ze zostało wykradzione i odczytane przez osobę nieuprawniona



Źródło: opracowanie własne na podstawie badań własnych

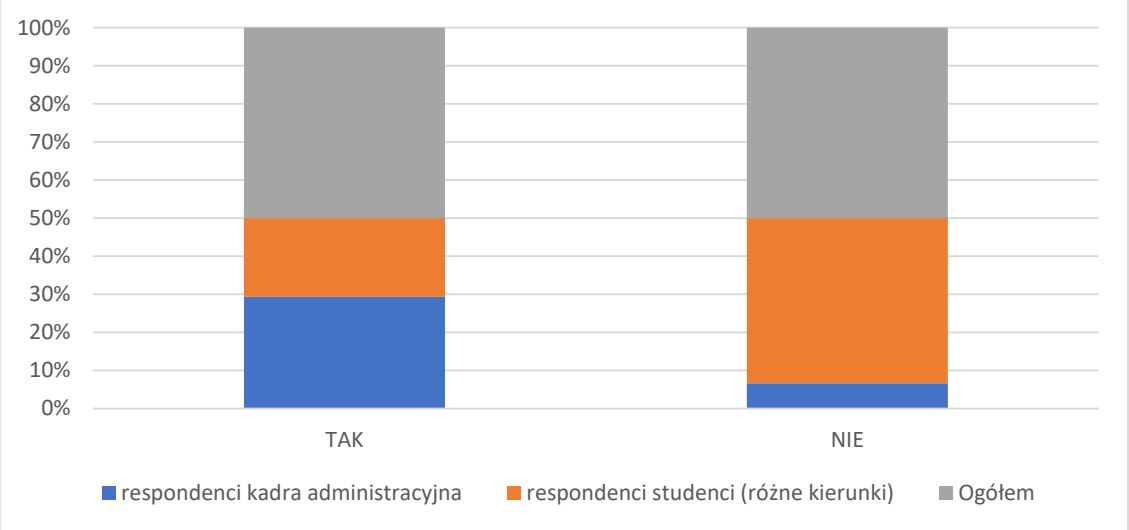
Wnioskować należy, że zarówno studenci jak i pracownicy naukowi starają się przekazywać informacje w razie utraty hasła lub podejrzenia, że zostało odczytane/wykradzione przez osobę nieuprawnioną. Rozkład odpowiedzi na temat informowania administratora uczelnianego systemu w przypadku utraty hasła lub podejrzenia, że zostało odczytane/wykradzione przez osobę nieuprawnioną wśród grupy kadry administracyjnej i grupy studentów (różne roczniki) zaprezentowano w tabeli 4.9.

Tabela 4.9. Odpowiedzi respondentów grupy kadra administracyjna i grupy studenci na temat informowania administratora przez użytkowników uczelnianego sytemu w przypadku utraty hasła lub podejrzenia, że zostało wykradzione i odczytane przez osobę nieuprawnioną

Odpowiedzi badanych osób **Informowanie administratora przez użytkowników uczelnianego systemu w przypadku utraty hasła lub podejrzenia, że zostało odczytane/wykorzystane przez osobę nieuprawnioną**							
Osoby poddane badaniu		**Respondenci kadra administracyjna**		**Respondenci studenci (różne kierunki)**		**OGÓŁEM**	
Ocena		*liczba wskazań*	*liczba wskazań*	*liczba wskazań*	*udział procentowy*	*liczba wskazań*	*udział procentowy*
TAK	**KOBIETY**	440	88%	251	50,2%	691	69,1%
	MĘŻCZYŹNI	35	7%	84	16,8%	119	11,9%
NIE	**KOBIETY**	18	3,6%	130	26%	148	14,8%
	MĘŻCZYŹNI	7	1,4%	35	7%	42	4,2%
		500	**500**	**500**	**100%**	**1000**	**100%**

Źródło: opracowanie własne na podstawie badań własnych

Wykres 4.17. Odpowiedzi respondentów grupy kadra administracyjna i grupy studenci (różne kierunki) na temat informowania administratora przez użytkowników uczelnianego sytemu w przypadku utraty hasła lub podejrzenia, że zostało wykradzione i odczytane przez osobę nieuprawnioną



Źródło: opracowanie własne na podstawie badań własnych

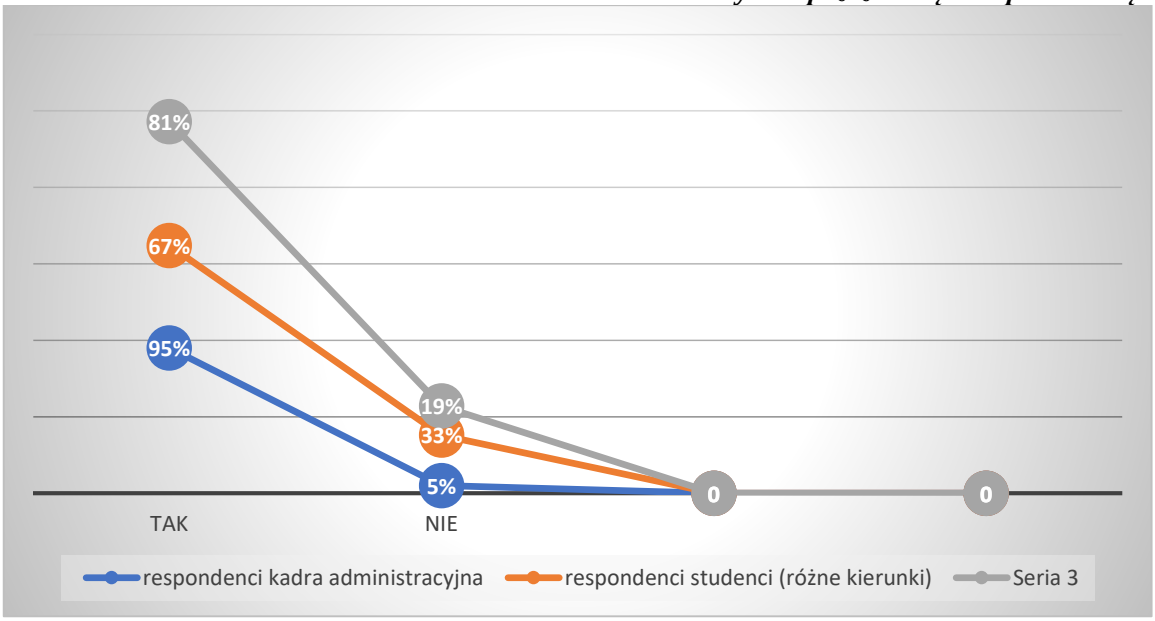
Badania empiryczne pokazały, że wśród kadry administracyjnej 95% respondentów zadeklarowało fakt, iż w przypadku utraty hasła lub podejrzenia, że zostało wykradzione i odczytane przez osobę nieuprawnioną zgłasza takie naruszenie. W tym jest 88% kobiet i 7% mężczyzn. Grupa studentów także deklaruje zgłoszenie takiego naruszenia, jednakże jest grupa respondentów, która zadeklarowała, że nie zgłasza tego faktu nikomu. Ogółem jest to 33% respondentów, w tym 26% kobiet i 7% mężczyzn.

Współczynnik korelacji liniowej Pearsona jest na poziomie 0,92 i współczynnik determinacji liniowej, który przedstawia procent wyjaśnionej liniowo zmienności wynosi 84,64%.

$$r_{xy} = \frac{\frac{1}{n}\sum_{i=1}^{n}(x_i-\bar{x})(y_i-\bar{y})}{s_x s_y}=0{,}92$$

$$\mathrm{WD}=r_{xy}^{2} * 100\% = 84{,}64\%$$

Wykres 4.18 Zależności między respondentami grupy kadra administracyjna i grupy studenci (różne kierunki) pod względem informowania administratora przez użytkowników uczelnianego systemu w przypadku utraty hasła lub podejrzenia, ze zostało wykradzione i odczytane przez osobę nieuprawnioną



Źródło: opracowanie własne na podstawie badań własnych

Deklaracje kadry administracyjnej wskazuję na przekaz informacji w uczelni wyższej o utracie hasła lub podejrzeniu, że zostało wykradzione i odczytane przez osobę do tego nieuprawnioną. Studenci, jako respondenci w większości deklarują też takie zachowanie w razie gdyby taka sytuacja się pojawiła.

Uogólniając, kadra administracyjna, jako grupa pracowników uczelnianych w 95% zadeklarowała zgłoszenie takiej sytuacji w razie jej wystąpienia. Pozostałe grupy przyznały, że nie wszyscy takie informacje przekazują administratorowi/dyrektorowi/opiekunowi konkretnej jednostki. Te same spostrzeżenia potwierdza przeprowadzona obserwacja uczestnicząca a także opinia eksperta. Z pozyskanych danych wynika, że kobiety w większym stopniu uczestniczą w życiu uczelni a tym samym korzystają ze szkolnego systemu informacyjnego.

Osoby, które wypowiedziały się przecząco to kobiety, nie dostrzegają one konieczności informowania administratora w uczelni wyższej w przypadku utraty hasła, co może mieć podłoże bardzo niskiej świadomości potencjalnych zagrożeń i bagatelizowania powstałego problemu. Jak widać z przeprowadzonych badań mężczyźni są bardziej wyczuleni na tego typu sytuacje.

W ramach koncepcji bezpieczeństwa systemu informacyjnego w uczelni wyższej powinna być w systemie wewnętrznym zakładka pozwalająca na zgłoszenie problemu a interwencja takiego działania powinna mieć rangę priorytetową, rejestrowaną i w systemie powinna być adnotacja, na jakim etapie załatwienia danej sprawy się znajduje. Powinna być także możliwość dopisywania komentarzy w razie konieczności lub uszczegółowienia już wcześniej przekazanych informacji.

Oceniając dla użytkownika możliwość poinformowania administratora uczelnianego systemu informacyjnego drogą elektroniczną w tym samym systemie, na którym docelowo pracuje przyczyni się, że z tej funkcji użytkownik będzie częściej i chętniej korzystał. Trudno jest szukać bezpośrednio kogoś czy też na piśmie zgłaszać problem w przypadku utraty hasła lub podejrzenia, że zostało ono odczytane bądź wykradzione przez osobę nieupoważnioną. Ponadto informacje wysyłane bezpośrednio do administratora nie powinny się pojawiać podglądowo w systemach dla wszystkich pracowników powinna być możliwość wybrania opcji „ komentarz prywatny".

Zwykle użytkownicy są zniechęceni szerszymi procedurami związanymi ze zgłaszaniem takich sytuacji bagatelizują problem. Koncepcja musi uwzględnić cechy społeczeństwa informacyjnego, ponieważ czasy teraźniejsze pokazują, że wszystkie działania załatwiane są za pośrednictwem sieci, narzędzi do przekazywania informacji. Informacje przesyłane w systemie przetrwają dłużej niż informacje wypowiedziane. Społeczeństwo w przypadku zaoszczędzenia, chociaż odrobiny czasu najchętniej korzysta z zaproponowanych możliwości wyboru systemów konkretnie przeznaczonych do danego procesu.

W badaniach empirycznych ocenie poddano ***czy użytkownicy systemu uczelni wyższej po zalogowaniu dokonują sprawdzania wiarygodności informacji odnośnie swojego ostatniego udanego logowania?*** Za pomocą sondażu diagnostycznego w ramach oceny poziomu bezpieczeństwa informacji przez respondentów grupy nauczyciele akademiccy i grupy kadra administracyjna mieli możliwość udzielenia jednej z dwóch zaproponowanych odpowiedzi „TAK", lub „NIE".

5. Czy dokonujecie Państwo po zalogowaniu sprawdzenia wiarygodności informacji odnośnie swojego ostatniego udanego logowania do systemu w uczelni wyższej?

Rozkład odpowiedzi respondentów grupy nauczyciele akademiccy i grupy kadra administracyjna dotyczący czy użytkownicy systemu uczelni wyższej po zalogowaniu dokonują sprawdzenia wiarygodności informacji odnośnie swojego ostatniego logowania prezentuje tabela 4.10.

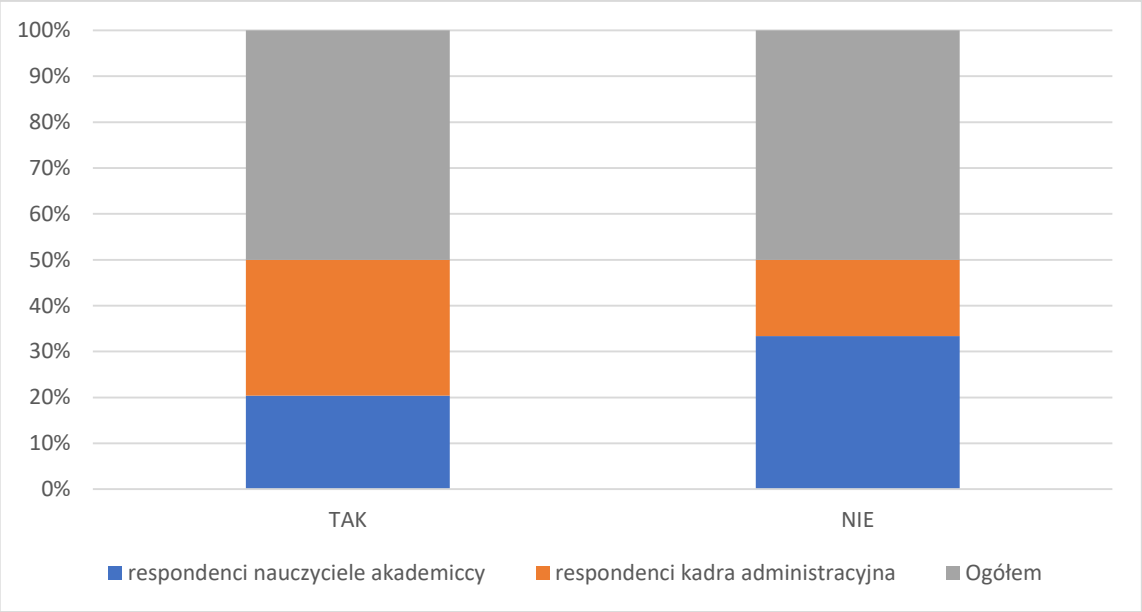
Tabela 4.10. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy kadra administracyjna na temat sprawdzenia wiarygodności informacji odnośnie swojego ostatniego udanego logowania do systemu uczelni wyższej

Odpowiedzi badanych osób Sprawdzenie wiarygodności informacji odnośnie swojego ostatniego udanego logowania do systemu uczelni wyższej						
Osoby poddane badaniu	**Respondenci nauczyciele akademiccy**		**Respondenci kadra administracyjna**		**OGÓŁEM**	
Ocena	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***
TAK	263	52,6%	382	76,4%	645	64,5%
NIE	237	47,4%	118	23,6%	355	35,5%
	500	**100%**	**500**	**100%**	**1000**	**100%**

Źródło: opracowanie własne na podstawie badań własnych

Odpowiedzi na pytanie 5 udzieliło 100% respondentów uczestniczących w badaniu. Odpowiedzi „ Tak" w grupie nauczycieli akademickich udzieliło 263 osób, co daje 52,6%. wśród kadry administracyjnej tą samą odpowiedź zadeklarowało 382 respondentów w udziale procentowym daje to 76,4%. Respondenci zadeklarowali również, że nie sprawdzają wiarygodności informacji odnośnie swojego ostatniego udanego logowania do systemu uczelni wyższej i wśród nauczycieli akademickich odpowiedź „Nie" wybrało 237 osób, co w przeliczeniu procentowym daje 47,4%, zaś przy respondentach grupy kadry administracyjnej taką deklarację złożyło 118 osób i jest to 23,6% w udziale procentowym.

Wykres 4.19. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy kadra administracyjna na temat sprawdzenia wiarygodności informacji odnośnie swojego ostatniego udanego logowania do sytemu uczelni wyższej



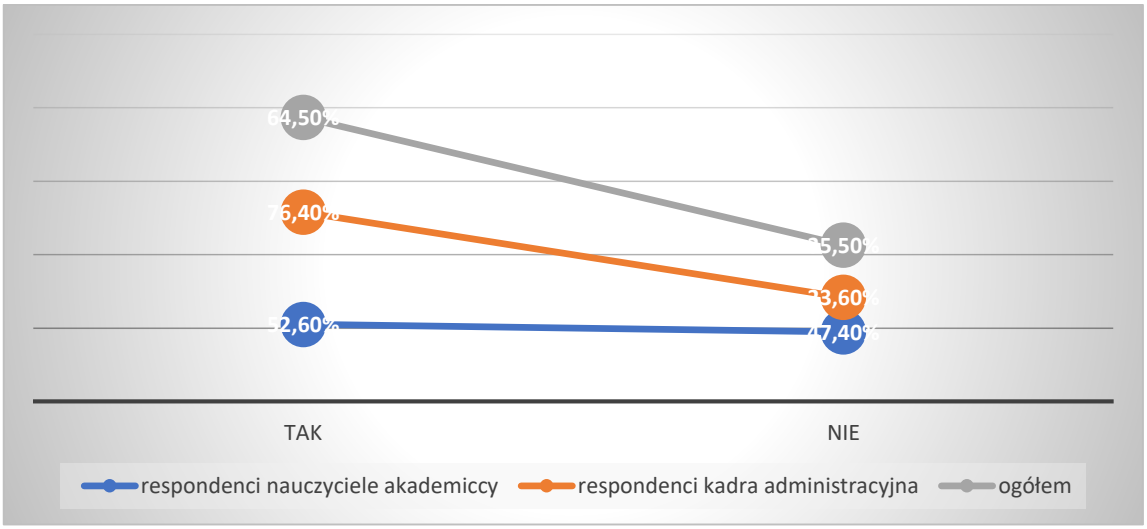
Źródło: opracowanie własne na podstawie badań własnych

Rozkład odpowiedzi, które zostały udzielone na pytanie dotyczące sprawdzenia wiarygodności informacji odnośnie swojego ostatniego logowania wskazują, że w grupie badawczej kadry administracyjnej to więcej osób dokonuje przedmiotowego sprawdzenia niż wśród osób grupy nauczycieli akademickich. O zależności świadczy współczynnik korelacji liniowej Pearsona na poziomie 1 i współczynnik determinacji liniowej, który wskazuje procent wyjaśnionej liniowo zmienności jest równy 100%.

$$r_{xy} = \frac{\frac{1}{n}\sum_{i=1}^{n}(x_i-\bar{x})(y_i-\bar{y})}{S_x S_y}=1$$

$$\text{WD}=r_{xy}^{2} * 100\% = 100\%$$

Wykres 4.20. Zależność między respondentami grupy nauczyciele akademiccy i grupy kadra administracyjna pod względem sprawdzania wiarygodności informacji odnośnie swojego ostatniego udanego logowania do systemu uczelni wyższej



Źródło: opracowanie własne na podstawie badań własnych

Uogólniając należy stwierdzić, że pracownicy naukowi jak i kadra administracyjna nie w pełni sprawdza swoje konta pod względem wiarygodności informacji odnośnie swojego ostatniego udanego logowania do systemu w uczelni wyższej. W tabeli 4.11. został zaprezentowany rozkład odpowiedzi grup nauczycieli akademickich i grupy studentów (różne kierunki) dokonujących odpowiedzi na pytanie czy użytkownicy systemu w uczelni wyższej po zalogowaniu dokonują sprawdzenia wiarygodności informacji odnośnie swojego ostatniego udanego logowania.

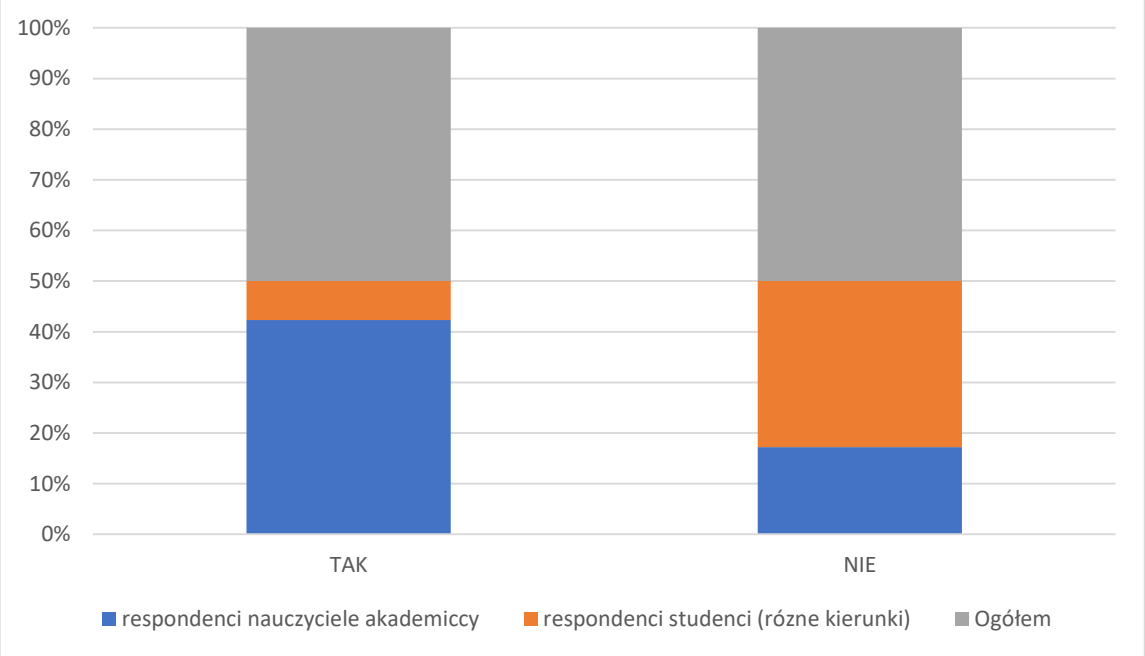
Tabela 4.11. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy studenci (różne kierunki) na temat sprawdzenia wiarygodności informacji odnośnie swojego ostatniego udanego logowania do systemu uczelni wyższej

Odpowiedzi badanych osób Sprawdzenie wiarygodności informacji odnośnie swojego ostatniego udanego logowania do systemu uczelni wyższej						
Osoby poddane badaniu	**Respondenci nauczyciele akademiccy**		**Respondenci studenci (różne kierunki)**		**OGÓŁEM**	
Ocena	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***
TAK	263	52,6%	48	9,6%	311	31,1%
NIE	237	47,4%	452	90,4%	689	68,9%
	500	**100%**	**500**	**100%**	**1000**	**100%**

Źródło: opracowanie własne na podstawie badań własnych

Z oceny uzyskanych wyników badań wynika, że wśród respondentów studentów (różnych kierunków) to 48 osób zadeklarowało, że sprawdza wiarygodność informacji odnośnie swojego ostatniego logowania do sytemu w uczelni wyższej. W udziale procentowym jest to 9,6%. Jednakże większa ilość respondentów w grupie studentów zadeklarowała, że nie sprawdza wiarygodności informacji odnośnie logowania i jest to 90,4% respondentów.

Wykres 4.21. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy studenci (różne kierunki) na temat sprawdzania wiarygodności informacji odnośnie swojego ostatniego udanego logowania do systemu w uczelni wyższej



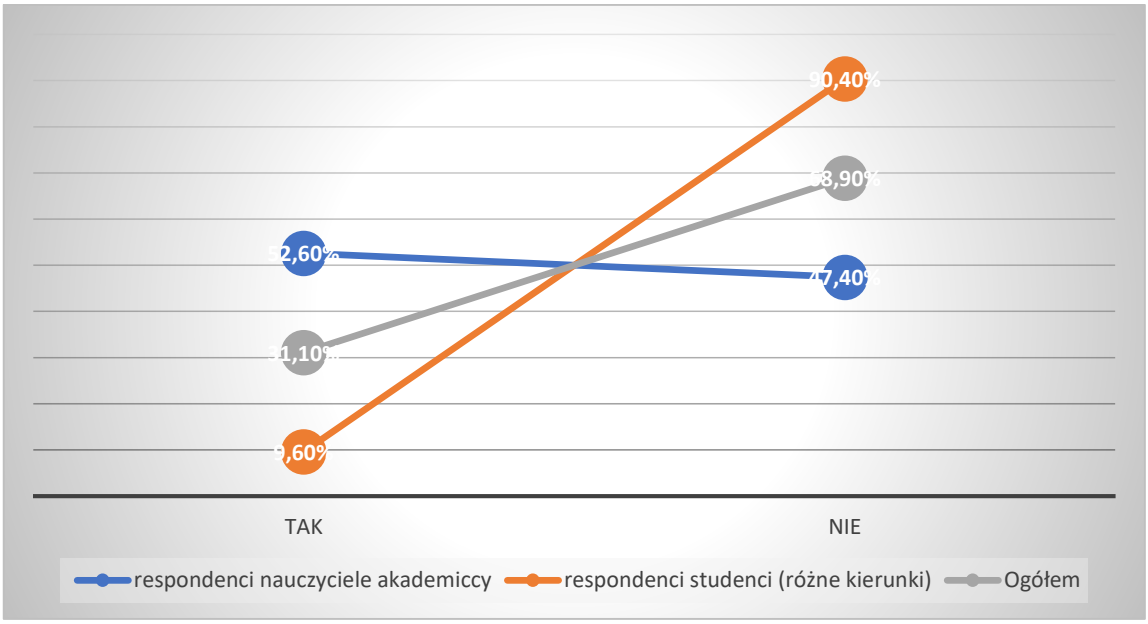
Źródło: opracowanie własne na podstawie badań własnych

Otrzymany współczynnik korelacji liniowej Pearsona klasuje się na poziomie -1 a współczynnik determinacji liniowej, który wskazuje procent wyjaśnionej liniowo zmienności jest równy 100%.

$$r_{xy} = \frac{\frac{1}{n}\sum_{i=1}^{n}(x_i-\bar{x})(y_i-\bar{y})}{S_x S_y}=-1$$

$$\mathrm{WD}=r_{xy}^{2} * 100\% = 100\%$$

Wykres 4.22. Zależność między respondentami grupy nauczyciele akademiccy i grupy studenci (różne kierunki) pod względem sprawdzenia wiarygodności informacji odnośnie swojego udanego logowania do systemu w uczelni wyższej



Źródło: Opracowanie własne na podstawie badań własnych

Uogólniając, wraz ze spadkiem wartości wśród nauczycieli akademickich rosną wartości wśród studentów (różnych kierunków), co oznacza bardzo silną korelację ujemną. Gdy nauczyciele akademiccy dokonują sprawdzenia ostatniego logowania do systemu, w grupie studentów zdecydowana większość pomija tę praktykę.

W tabeli 4.12. zostały rozmieszczone odpowiedzi na temat dokonywania po zalogowaniu sprawdzenia wiarygodności informacji odnośnie swojego ostatniego udanego logowania wśród grupy respondentów, jaką jest kadra administracyjna i grupy studentów (różnych kierunków).

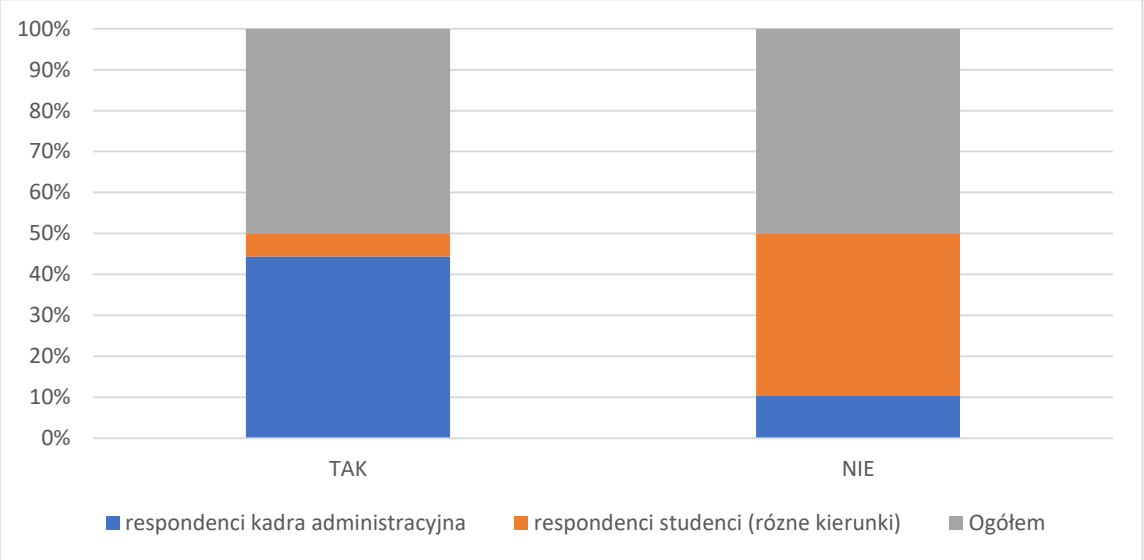
Tabela 4.12. Odpowiedzi respondentów grupy kadra administracyjna i grupy studenci (różne kierunki) na temat sprawdzania wiarygodności informacji odnośnie swojego ostatniego logowania do systemu uczelni wyższej

Odpowiedzi badanych osób Sprawdzenie wiarygodności informacji odnośnie swojego ostatniego udanego logowania do systemu uczelni wyższej						
Osoby poddane badaniu	**Respondenci kadra administracyjna**		**Respondenci studenci (różne kierunki)**		**OGÓŁEM**	
Ocena	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***
TAK	382	76,4%	48	9,6%	430	43%
NIE	118	23,6%	452	90,4%	570	57%
	500	**100%**	**500**	**100%**	**1000**	**100%**

Źródło: opracowanie własne na podstawie badań własnych

W ramach przeprowadzonych badań, według opinii respondentów 76,4% kadry administracyjnej dokonuje sprawdzenia wiarygodności informacji odnośnie swojego ostatniego udanego logowania do systemu w uczelni wyższej. W przypadku studentów jest to zaledwie 9,6% osób. Brak logowania wśród kadry administracyjnej deklaruje 23,6% respondentów, zaś w grupie studentów tą odpowiedź zadeklarowało 90,4% osób.

Wykres 4.23. Odpowiedzi respondentów grupa kadra administracyjna i grupy studenci (różne kierunki) na temat sprawdzenia wiarygodności informacji odnośnie swojego ostatniego udanego logowania do systemu w uczelni wyższej



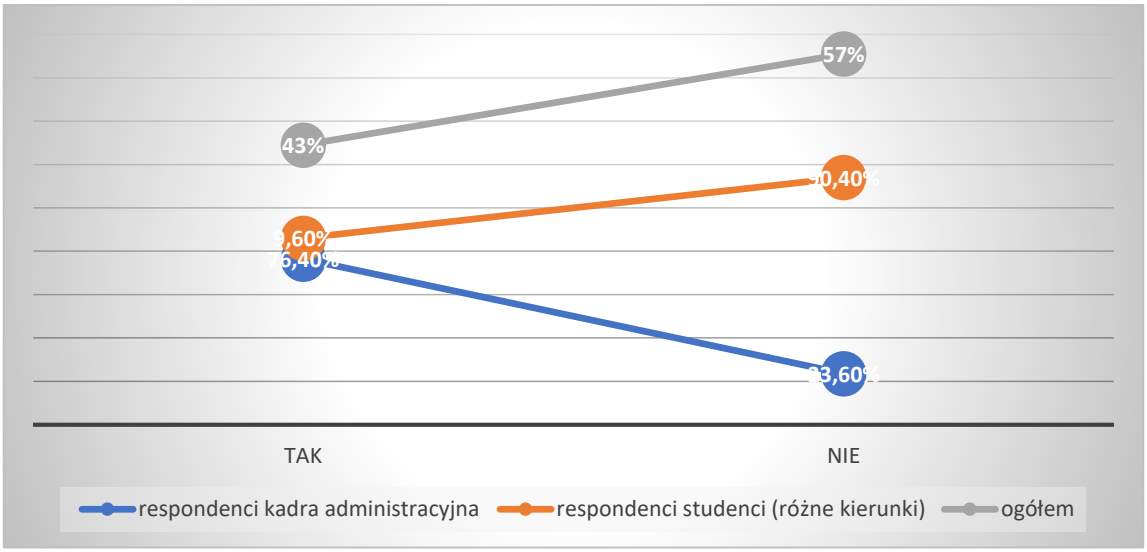
Źródło: opracowanie własne na podstawie badań własnych

Wraz ze spadkiem wartości wśród kadry administracyjnej rosną wartości wśród studentów (różnych kierunków), co oznacza bardzo silną korelację ujemną. Potwierdza to fakt, że kadra administracyjna dokonuje sprawdzenia ostatniego logowania do systemu, zaś studenci zdecydowanie unikają takiego procesu. Świadczy o tym współczynnik korelacji liniowej Pearsona na poziomie -1 i współczynnik determinacji liniowej, który wskazuje procent wyjaśnionej liniowo zmienności równej 100%.

$$r_{xy} = \frac{\frac{1}{n}\sum_{i=1}^{n}(x_i-\bar{x})(y_i-\bar{y})}{S_x S_y}=-1$$

$$\mathrm{WD}=r_{xy}^{2} * 100\% = 100\%$$

Wykres 4.24. Zależność między respondentami grupy kadra administracyjna i grupy studenci (różne kierunki) pod względem sprawdzania wiarygodności informacji odnośnie swojego ostatniego udanego logowania do systemu w uczelni wyższej



*Źródło: opracowanie własne na podstawie badań wł*asnych

Dokonując podsumowania należy wskazać, że w każdej z grup respondentów znajdują się osoby, które po zalogowaniu się do systemu nie sprawdzają wiarygodności informacji odnośnie swojego ostatniego udanego logowania. Zdecydowana większość studentów loguje się do systemu bez weryfikacji jego bezpieczeństwa. Wśród odpowiedzi pracowników uczelni wyższej poddanym badaniom, jakimi byli nauczyciele akademiccy i kadra administracyjna pojawiły się odpowiedzi pozytywne (twierdzące), które w domyśle były nieprawdziwe, zgodnie ze stanem faktycznym występującym w uczelni wyższej. Spowodowało to przedstawienie błędnego obrazu zachowań użytkowników systemu, których obserwacja i ocena eksperta wskazuje, że mało, kto z użytkowników poddanych badaniu praktykuje weryfikację ostatniego logowania.

Z obserwacji wynika, że pracownicy najczęściej logują się do systemu, odruchowo z pełną rutyną, spontanicznie i szybko, gdyż natłok spraw powoduje, że każdy się spieszy, aby zrealizować powierzone mu przez przełożonych obowiązki. W pewnym sensie zostaje wyłączona kontrola mająca na celu ustrzec przed popełnieniem błędu. Jednakże realia codzienności są inne niż czasami można sobie je wyobrazić.

Wprowadzona koncepcja bezpieczeństwa powinna w pewnym stopniu wymusić na pracowniku pewien proces. Po zalogowaniu do sytemu powinna pojawić się przypominająca informacja (wymuszająca) na użytkowniku konieczność sprawdzenia informa-

cji dotyczącej ostatniego logowania a następnie po jej zatwierdzeniu będzie można wykonywać dalsze czynności. Wskazana powyżej sytuacja doprowadziłaby do zwiększenia czujności, wrażliwości i nawyku oraz skłoniło do weryfikacji wszelkiego rodzaju logowań do wewnętrznego systemu uczelni wyższej. W badaniach empirycznych pojawiło się pytanie ***czy w przypadku stwierdzenia przez Państwa nieścisłości na koncie w systemie, osobiście o tym fakcie informujecie administratora uczelnianego odpowiedzialnego za system informacyjny?*** Za pomocą sondażu diagnostycznego w ramach oceny poziomu bezpieczeństwa informacji przez respondentów grupy nauczycieli akademickich, grupy kadra administracyjna, grupy studenci (różne kierunki) ankietowani mieli możliwość udzielenia jednej z dwóch zaproponowanych odpowiedzi „TAK", „NIE".

6. Czy w przypadku stwierdzenia przez Państwa nieścisłości na koncie w systemie, osobiście o tym fakcie informujecie administratora uczelnianego odpowiedzialnego za system informacyjny?

Rozkład odpowiedzi udzielonych przez respondentów grupy nauczyciele akademiccy i grupy kadra administracyjna został zaprezentowany w tabeli 4.13.

Tabela 4.13. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy kadra administracyjna na temat osobistego informowania uczelnianego administratora odpowiedzialnego za system informacyjny o fakcie stwierdzenia nieścisłości na swoim koncie w systemie

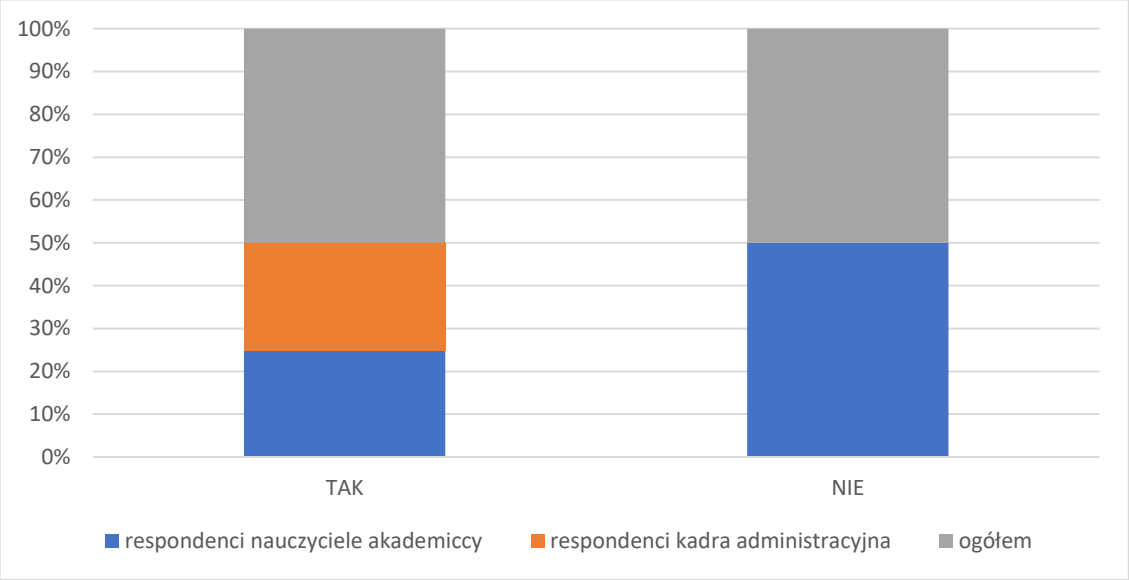
Odpowiedzi badanych osób Osobiste informowanie uczelnianego administratora odpowiedzialnego za system informacyjny?						
Osoby poddane badaniu	**Respondenci nauczyciele akademiccy**		**Respondenci kadra administracyjna**		**OGÓŁEM**	
Ocena	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***
TAK	490	98%	500	100%	990	99%
NIE	10	2%	0	0%	10	1%
	500	**100%**	**500**	**100%**	**1000**	**100%**

Źródło: opracowanie własne na podstawie badań własnych

W badaniu wzięło udział 100% respondentów w każdej z grup badanych. Na pytanie dotyczące osobistego informowania uczelnianego administratora zajmującego się wirtualną uczelnią/USOS-em w sytuacji stwierdzenia nieścisłości na swoim koncie w systemie w grupie nauczycieli akademickich pozytywnie odpowiedziało 490 respondentów, co w udziale procentowym daje 98%. Kadra administracyjna wypowiedziała się

w 100% wskazując na osobiste informowanie uczelnianego admiratora w przypadku wystąpienia nieścisłości na koncie w systemie. Wśród respondentów grupy nauczycieli akademickich tylko 10 osób nie informuje osobiście uczelnianego administratora to daje w przeliczeniu procentowym 2%.

Wykres 4.25. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy kadra administracyjna na temat osobistego informowania uczelnianego administratora odpowiedzialnego za system informacyjny o fakcie stwierdzenia nieścisłości na swoim koncie w systemie



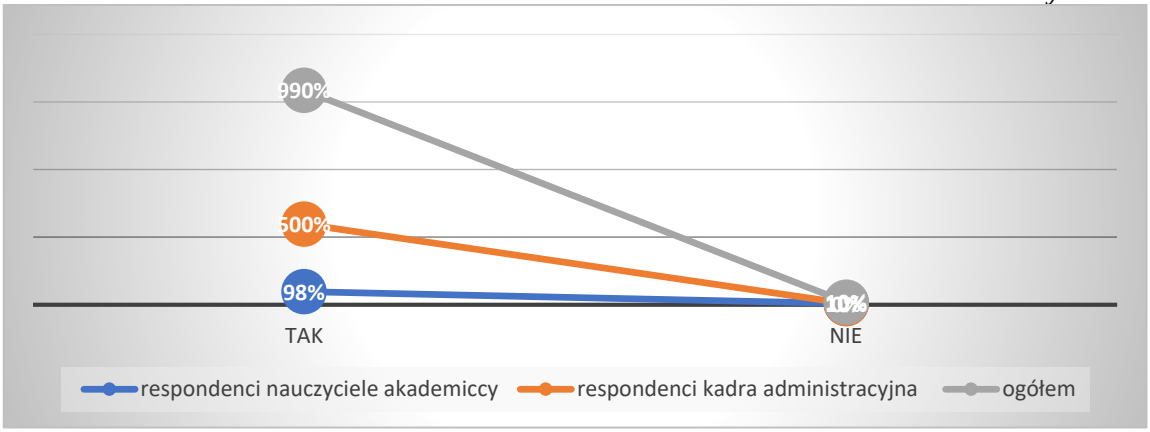
Źródło: opracowanie własne na podstawie badań własnych

O zależności miedzy zmiennymi świadczy współczynnik korelacji liniowej Pearsona na poziomie 1 i współczynnik determinacji liniowej, który wskazuje procent wyjaśnionej liniowo zmienności równy 100%.

$$r_{xy} = \frac{\frac{1}{n}\sum_{i=1}^{n}(x_i-\bar{x})(y_i-\bar{y})}{S_x S_y}=1$$

$$\text{WD}=r_{xy}^{2} * 100\% = 100\%$$

Wykres 4.26. Zależność miedzy respondentami grupy nauczyciele akademiccy i grupy kadra administracyjna pod względem osobistego informowania uczelnianego administratora odpowiedzialnego za system informacyjny o fakcie stwierdzenia nieścisłości na swoim koncie w systemie



Źródło: opracowanie własne na podstawie badań własnych

Uogólniając, wraz ze spadkiem wartości jednej grupy respondentów maleją wartości drugiej grupy respondentów, fakt ten oznacza bardzo silną korelację dodatnią. Widać wyraźnie, że zarówno nauczyciele akademiccy jak i kadra administracyjna deklarują osobiste informowanie administratora o nieprawidłowościach w systemie. Tabela 4.14. prezentuje rozkład odpowiedzi respondentów na postawione pytanie dotyczące osobistego informowania uczelnianego administratora zajmującego się wirtualną uczelnią/USOS-em o fakcie stwierdzenia nieprawidłowości na swoim koncie w systemie.

Tabela 4.14. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy studenci (różne kierunki) na temat osobistego informowania uczelnianego administratora odpowiedzialnego za system informacyjny o fakcie stwierdzenia nieścisłości na swoim koncie w systemie

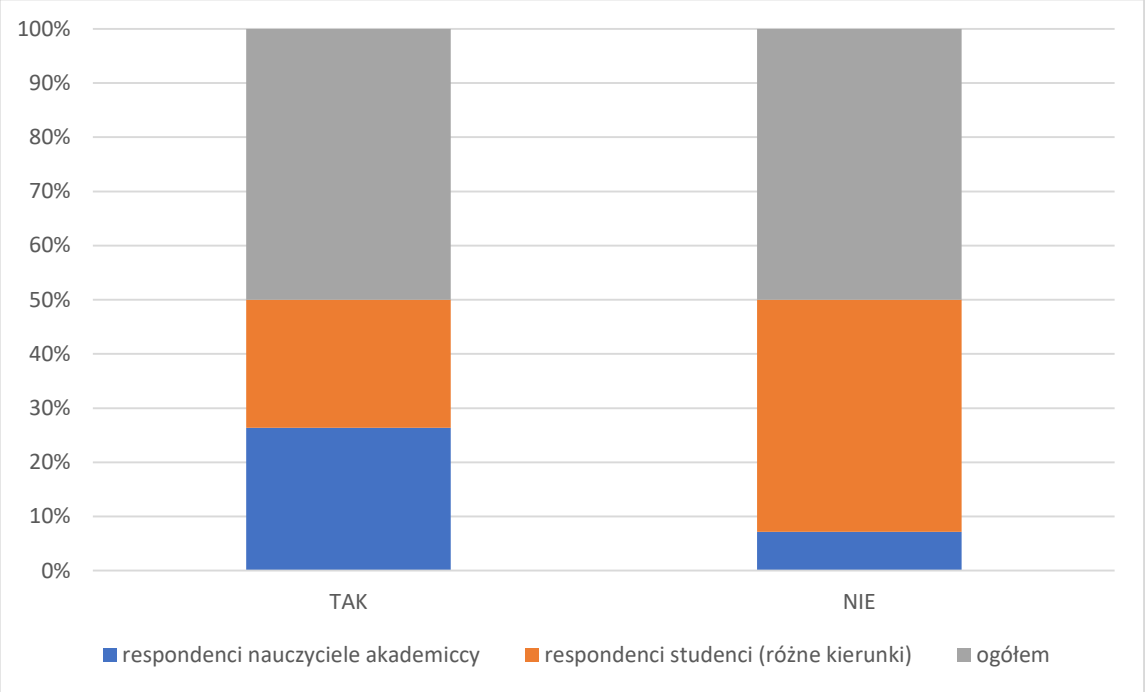
Odpowiedzi badanych osób Osobiste informowanie uczelnianego administratora odpowiedzialnego za system informacyjny?						
Osoby poddane badaniu	**Respondenci nauczyciele akademiccy**		**Respondenci studenci (różne kierunki)**		**OGÓŁEM**	
Ocena	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***
TAK	490	98%	440	88%	930	93%
NIE	10	2%	60	12%	70	7%
	500	**100%**	**500**	**100%**	**1000**	**100%**

Źródło: opracowanie własne na podstawie badań własnych

Wyniki wskazują, że wśród studentów (różnych kierunków), 440 respondentów zadeklarowało osobiste informowanie uczelnianego administratora o fakcie stwierdzenia

nieścisłości na swoim koncie w systemie, co daje w przeliczeniu procentowym 93%. Nie zgłaszanie incydentów wśród grupy studentów zadeklarowało 60 osób to daje 12%.

Wykres 4.27. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy studenci (różne kierunki) na temat osobistego informowania uczelnianego administratora odpowiedzialnego za system informacyjny o fakcie stwierdzenia nieścisłości na swoim koncie w systemie



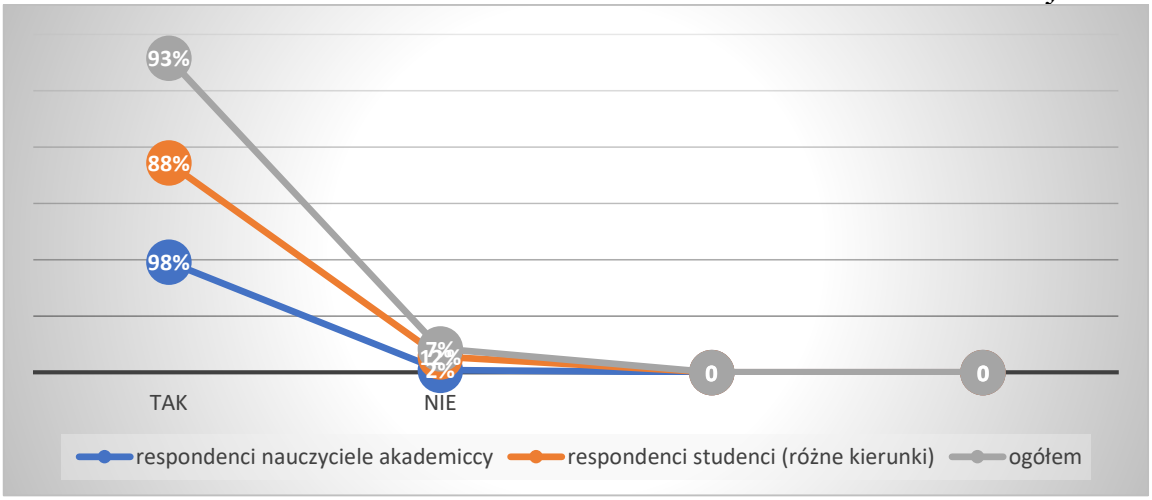
Źródło: opracowanie własne na podstawie badań własnych

Występuje zależność miedzy zmiennymi, o czym świadczy współczynnik korelacji liniowej Pearsona na poziomie 1 i współczynnik determinacji liniowej, który wskazuje procent wyjaśnionej liniowo zmienności równy 100%.

$$r_{xy} = \frac{\frac{1}{n}\sum_{i=1}^{n}(x_i-\bar{x})(y_i-\bar{y})}{S_x S_y}=1$$

$$\text{WD}=r\frac{2}{xy} * 100\% = 100\%$$

Wykres 4.28. Zależność między respondentami grupy nauczyciele akademiccy i grupy studenci (różne kierunki) pod względem osobistego informowania uczelnianego administratora odpowiedzialnego za system informacyjny o fakcie stwierdzenia nieścisłości na swoim koncie w systemie



Źródło: opracowanie własne na podstawie badań własnych

Powyższy rozkład odpowiedzi wskazuje, że wraz ze spadkiem wartości wśród jednej z grup maleją wartości wśród drugiej z grup. Wskazuje to na bardzo silną korelację dodatnią równą wartości progowej współczynnika korelacji liniowej Pearsona na poziomie 1. Nauczyciele akademiccy i studenci informują osobiście administratora uczelnianego o nieprawidłowościach na swoim koncie w systemie. Kolejna tabela 4.15. zawiera odpowiedzi grupy kadra administracyjna i studenci (różne kierunki) na temat osobistego informowania uczelnianego administratora zajmującego się wirtualną uczelnią/USOS-em o fakcie stwierdzenia nieprawidłowości na swoim koncie w systemie.

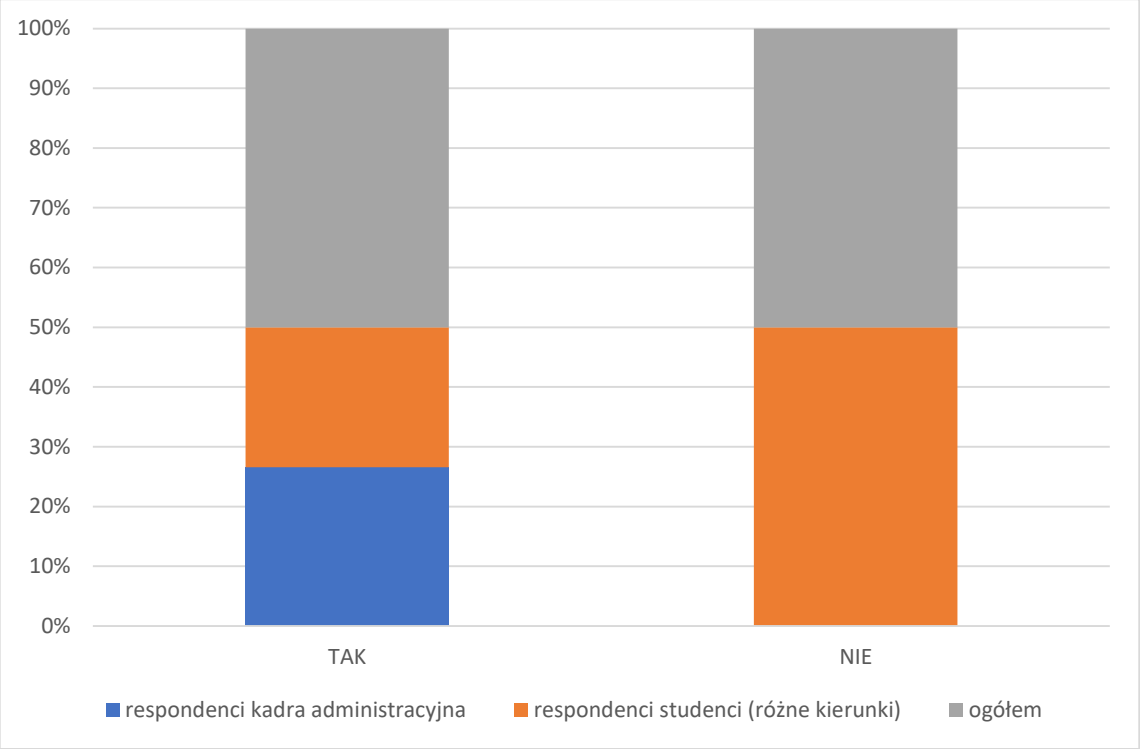
Tabela 4.15. Odpowiedzi respondentów grupy kadra administracyjna i grupy studenci (różne kierunki) na temat osobistego informowania uczelnianego administratora odpowiedzialnego za system informacyjny o fakcie stwierdzenia nieścisłości na swoim koncie w systemie

Odpowiedzi badanych osób Osobiste informowanie uczelnianego administratora odpowiedzialnego za system informacyjny?						
Osoby poddane badaniu	**Respondenci kadra administracyjna**		**Respondenci studenci (różne kierunki)**		**OGÓŁEM**	
Ocena	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***
TAK	500	100%	440	88%	940	94%
NIE	0	0%	60	12%	60	6%
	500	**100%**	**500**	**100%**	**1000**	**100%**

Źródło: opracowanie własne na podstawie badań własnych

Podsumowując wyniki widać, że 100% kadry administracyjnej deklaruje osobiste informowanie uczelnianego administratora zajmującego się wirtualną uczelnią/USOS-em o fakcie stwierdzenia nieprawidłowości na swoim koncie w systemie, zaś studenci w 88%. Respondenci grupy studentów w 12% nie informują o zauważalnych nieścisłościach.

Wykres 4.29. Odpowiedzi respondentów grupy kadra administracyjna i grupy studenci (różne kierunki) na temat osobistego informowania uczelnianego administratora odpowiedzialnego za system informacyjny o fakcie stwierdzenia nieścisłości na swoim koncie w systemie



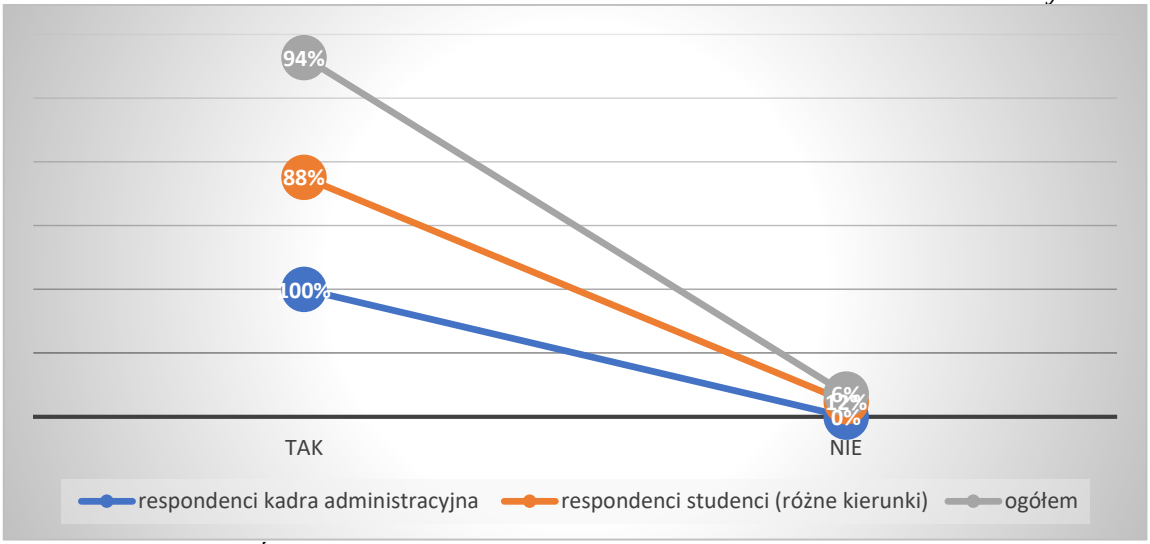
Źródło: opracowanie własne na podstawie badań własnych

O zależności świadczy współczynnik korelacji liniowej Pearsona na poziomie 1 i współczynnik determinacji liniowej, wskazuje procent wyjaśnionej liniowo zmienności równy 100%.

$$r_{xy} = \frac{\frac{1}{n}\sum_{i=1}^{n}(x_i-\bar{x})(y_i-\bar{y})}{S_x S_y}=1$$

$$\text{WD}=r_{xy}^{2} * 100\% = 100\%$$

Wykres 4.30. Zależność między respondentami grupy kadra administracyjna i grupy studenci (różne kierunki) na temat osobistego informowania uczelnianego administratora odpowiedzialnego za system informacyjny o fakcie stwierdzenia nieścisłości na swoim koncie w systemie



Źródło: opracowanie własne na podstawie badań własnych

Wnioskując, tylko pracownicy kadry administracyjnej w 100% zadeklarowali, że osobiście informują uczelnianego administratora zajmującego się wirtualną uczelnią/USOS-em o fakcie stwierdzenia nieprawidłowości na swoim koncie w systemie. W pozostałych grupach respondentów pojawiły się osoby, które deklarują, że nie informują osobiście powyżej wspomnianego administratora.

Często społeczność uczelniana musi się zmierzyć z faktem, że główny administrator nie przebywa codziennie fizycznie na terenie uczelni wyższej. Jego praca jest często w formie zdalnej. Stacjonarnie przebywają osoby, które tylko doraźnie mogą pomóc a otrzymana pomoc jest na chwilę. Ograniczony kontakt zniechęca użytkowników systemu do przestrzegania ustalonych procedur. Najbardziej utrudniony kontakt z takim administratorem mają studenci w dużej mierze są to kandydaci, którzy dopiero zostali zrekrutowani na kierunki proponowane przez uczelnię wyższą.

W ramach koncepcji bezpieczeństwa systemu informacyjnego należy wprowadzić możliwość informowania elektronicznego a nie w sposób bezpośredni. W obecnym czasie jest to najczęstszy kanał komunikacji respondentów pozwalający na szybkie i łatwe dotarcie do adresata i rozwiązanie zaistniałego problemu. W badaniach empirycznych ocenie poddano ***czy w przypadku korzystania z prywatnego komputera czy laptopa w dostępie do systemów wewnętrznych zachowują wszystkie zasady ochrony danych osobowych stosowane w uczelni wyższej?***. Za pomocą sondażu diagnostycznego w ramach

oceny poziomu bezpieczeństwa informacji przez respondentów grupy nauczyciele akademiccy, grupy kadra administracyjna, grupy studenci (różne kierunki). `Ankietowani mieli możliwość udzielenia jednej z dwóch zaproponowanych odpowiedzi „TAK" lub „NIE".

7. Czy w przypadku korzystania z prywatnego komputera lub laptopa w dostępie do systemów wewnętrznych zachowują Państwo wszystkie zasady ochrony danych osobowych stosowane w uczelni wyższej? Tabela 4.16. prezentuje rozkład odpowiedzi udzielonych przez respondentów grupy nauczyciele akademiccy i grupy kadra administracyjna dotyczących zachowania wszystkich zasad ochrony danych osobowych stosowanych w uczelni wyższej przez użytkowników w przypadku korzystania z prywatnego komputera lub laptopa w dostępie do systemów wewnętrznych.

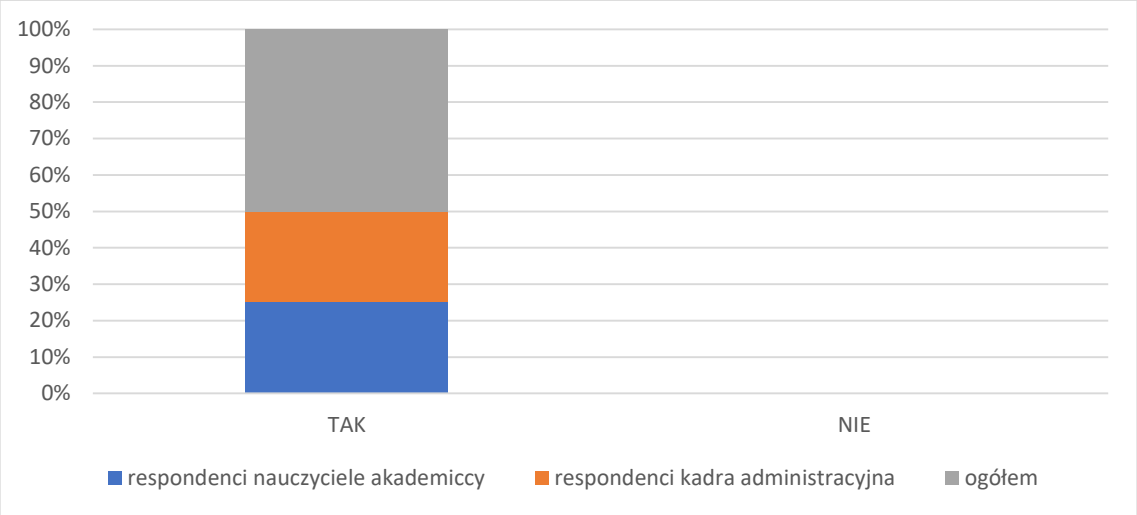
Tabela 4.16. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy kadra administracyjna na temat zachowania wszystkich zasad ochrony danych osobowych stosowanych w uczelni wyższej przez użytkowników w przypadku korzystania z prywatnego komputera lub laptopa w dostępie do systemów wewnętrznych

Odpowiedzi badanych osób Zachowanie wszystkich zasad ochrony danych osobowych stosowanych w uczelni wyższej przez użytkowników w przypadku korzystania z prywatnego komputera lub laptopa w dostępie do systemów wewnętrznych						
Osoby poddane badaniu	**Respondenci nauczyciele akademiccy**		**Respondenci kadra administracyjna**		**OGÓŁEM**	
Ocena	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***
TAK	500	100%	500	100%	1000	100%
NIE	0	0%	0	0%	0	0%
	500	**100%**	**500**	**100%**	**1000**	**100%**

Źródło: opracowanie własne na podstawie badań własnych

Ogółem odpowiedzi na pytanie 7 kwestionariusza ankiety dotyczące zachowania wszystkich zasad ochrony danych osobowych stosowanych w uczelni wyższej przez użytkowników w przypadku korzystania z prywatnego komputera lub laptopa w dostępie do systemów wewnętrznych udzieliło 100% respondentów z każdej z badanych grup. Z otrzymanego materiału empirycznego wynika, że zarówno grupa nauczycieli akademickich jak i grupa kadry administracyjnej zadeklarowała, w 100%, że zachowuje wszystkie zasady ochrony danych osobowych stosowanych w uczelni wyższej przez użytkowników w przypadku korzystania z prywatnego komputera lub laptopa w dostępie do systemów wewnętrznych.

Wykres 4.31. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy kadra administracyjna na temat zachowania wszystkich zasad ochrony danych osobowych stosowanych w uczelni wyższej przez użytkowników w przypadku korzystania z prywatnego komputera lub laptopa w dostępie do systemów wewnętrznych



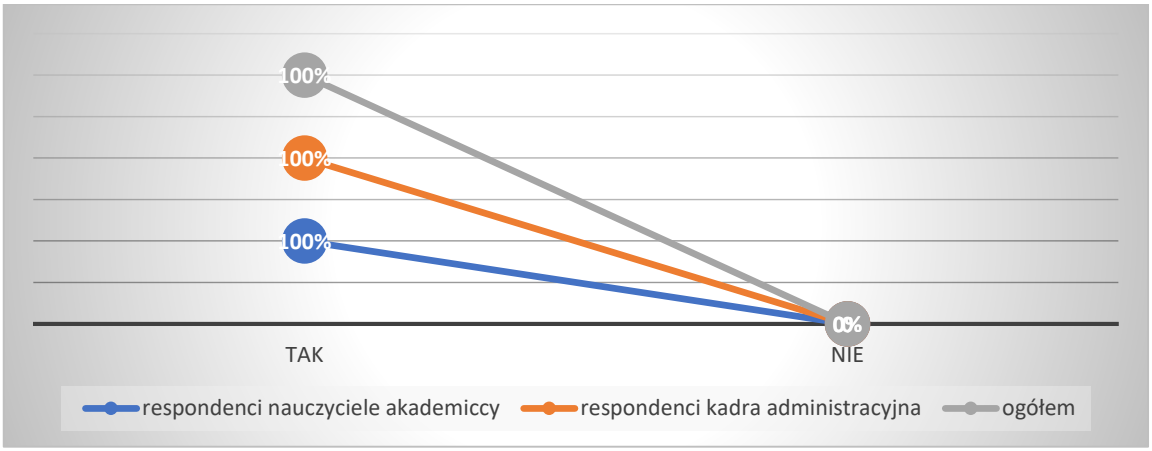
Źródło: opracowanie własne na podstawie badań własnych

Występuje zależność pomiędzy zmiennymi, o czym świadczy współczynnik korelacji liniowej Pearsona na poziomie 1 i współczynnik determinacji liniowej, który wskazuje procent wyjaśnionej liniowo zmienności równy 100%.

$$r_{xy} = \frac{\frac{1}{n}\sum_{i=1}^{n}(x_i-\bar{x})(y_i-\bar{y})}{S_x S_y}=1$$

$$\mathrm{WD}=r_{xy}^{2} * 100\% = 100\%$$

Wykres 4.32. Zależność między respondentami grupy nauczyciele akademiccy i grupy kadra administracyjna pod względem zachowania wszystkich zasad ochrony danych osobowych stosowanych w uczelni wyższej przez użytkowników w przypadku korzystania z prywatnego komputera lub laptopa w dostępie do systemów wewnętrznych



Źródło: opracowanie własne na podstawie badań własnych

Uogólniając widać, że wraz ze spadkiem wartości wśród grupy nauczycieli akademickich maleją wartości wśród grupy kadra administracyjna, oznacza to bardzo silną korelację dodatnią. W opinii nauczycieli akademickich i kadry administracyjnej są zachowane przez obie grupy respondentów zasady ochrony podczas logowania się do uczelnianych systemów z prywatnego komputera. Tabela 4.17 przedstawia odpowiedzi respondentów na temat zachowania wszystkich zasad ochrony danych osobowych stosowanych w uczelni wyższej przez użytkowników w przypadku korzystania z prywatnego komputera lub laptopa w dostępie do systemów wewnętrznych

Tabela 4.17. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy studenci (różne kierunki) na temat zachowania wszystkich zasad ochrony danych osobowych stosowanych w uczelni wyższej przez użytkowników w przypadku korzystania z prywatnego komputera lub laptopa w dostępie do systemów wewnętrznych

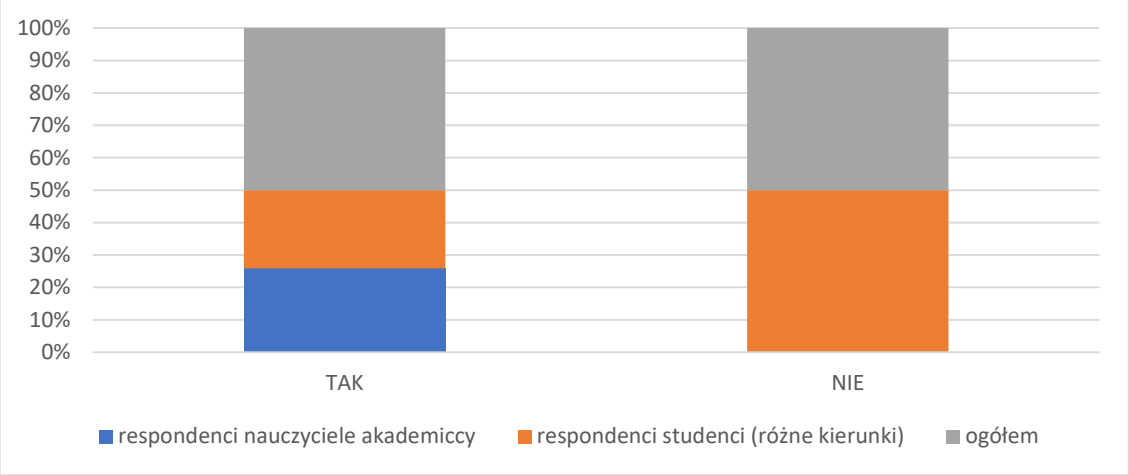
Odpowiedzi badanych osób Zachowanie wszystkich zasad ochrony danych osobowych stosowanych w uczelni wyższej przez użytkowników w przypadku korzystania z prywatnego komputera lub laptopa w dostępie do systemów wewnętrznych						
Osoby poddane badaniu	**Respondenci nauczyciele akademiccy**		**Respondenci studenci (różne kierunki)**		**OGÓŁEM**	
Ocena	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***
TAK	500	100%	465	93%	965	96,5%
NIE	0	0%	35	7%	35	3,5%
	500	**100%**	**500**	**100%**	**1000**	**100%**

Źródło: opracowanie własne na podstawie badań własnych

W opinii 465 respondentów w grupie studentów, co daje w przeliczeniu procentowym 93%, zachowane są wszystkie zasady ochrony danych osobowych stosowanych w uczelni wyższej przez użytkowników w przypadku korzystania z prywatnego komputera lub laptopa w dostępie do systemów wewnętrznych.

Negatywnej odpowiedzi udzieliło w powyższym pytaniu 35 osób z tej grupy, co daje w przeliczeniu procentowym 7%.

Wykres 4.33 Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy studenci (różne kierunki) na temat zachowania wszystkich zasad ochrony danych osobowych stosowanych w uczelni wyższej przez użytkowników w przypadku korzystania z prywatnego komputera lub laptopa w dostępie do systemów wewnętrznych



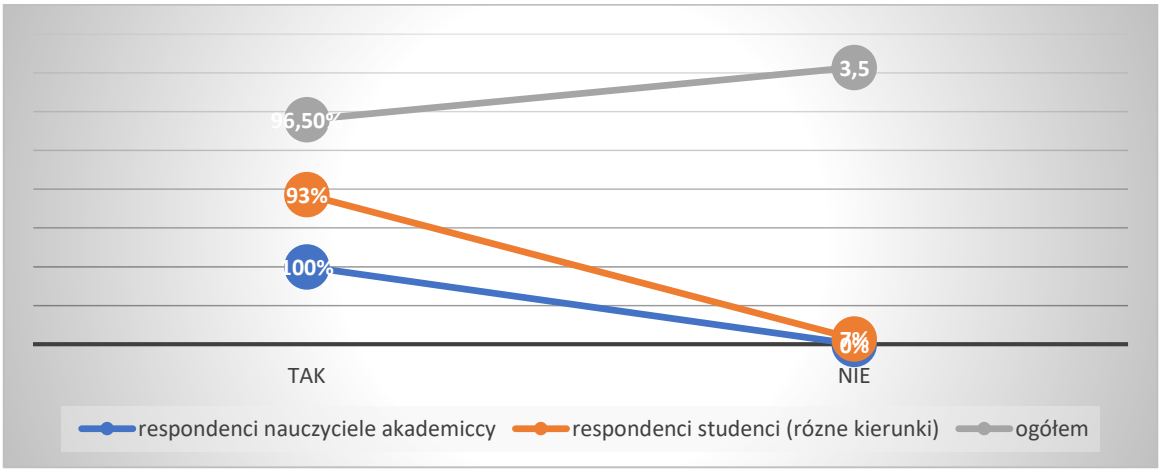
Źródło: opracowanie własne na podstawie badań własnych

Istnieje zależność pomiędzy zmiennymi, o czym świadczy współczynnik korelacji liniowej Pearsona na poziomie 1 i współczynnik determinacji liniowej, który wskazuje procent wyjaśnionej liniowo zmienności i jest równy 100%.

$$r_{xy} = \frac{\frac{1}{n}\sum_{i=1}^{n}(x_i-\bar{x})(y_i-\bar{y})}{S_x S_y}=1$$

$$\text{WD}=r_{xy}^{2} * 100\% = 100\%$$

Wykres 4.34. Zależność między respondentami grupy nauczyciele akademiccy i grupy studenci (różne kierunki) pod względem zachowania wszystkich zasad ochrony danych osobowych stosowanych w uczelni wyższej przez użytkowników w przypadku korzystania z prywatnego komputera lub laptopa w dostępie do systemów wewnętrznych



Źródło: opracowanie własne na podstawie badań własnych

Powyższy rozkład wskazuje na fakt, że wraz ze spadkiem wartości wśród grupy nauczycieli akademickich maleją wartości wśród studentów, co pozwala wnioskować na bardzo silną korelację dodatnią równą wartości progowej współczynnika korelacji liniowej Pearsona na poziomie 1. Według opinii grupy nauczycieli akademickich i grupy studentów (różnych kierunków) są przestrzegane standardy pracy z korzystaniem z wewnętrznych systemów, komputerów prywatnych. W tabeli 4.18. zostały rozmieszczone odpowiedzi grupy kadra administracyjna i studenci (różne kierunki) na temat zachowania wszystkich zasad ochrony danych osobowych stosowanych w uczelni wyższej przez użytkowników w przypadku korzystania z prywatnego komputera lub laptopa w dostępie do systemów wewnętrznych.

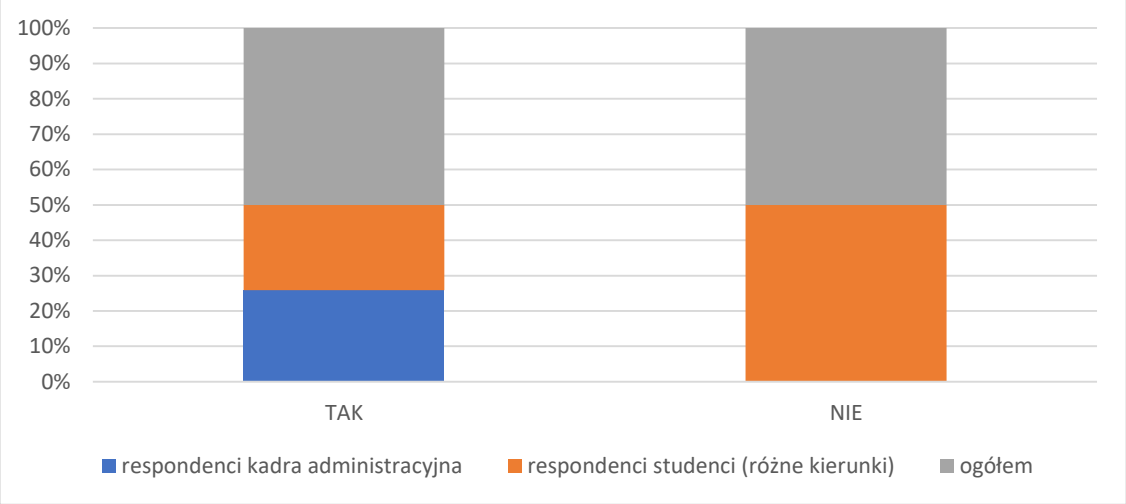
Tabela 4.18. Odpowiedzi respondentów grupy kadra administracyjna i grupy studenci (różne kierunki) na temat zachowania wszystkich zasad ochrony danych osobowych stosowanych w uczelni wyższej przez użytkowników w przypadku korzystania z prywatnego komputera lub laptopa w dostępie do systemów wewnętrznych

Odpowiedzi badanych osób Zachowanie wszystkich zasad ochrony danych osobowych stosowanych w uczelni wyższej przez użytkowników w przypadku korzystania z prywatnego komputera lub laptopa w dostępie do systemów wewnętrznych						
Osoby poddane badaniu	**Respondenci kadra administracyjna**		**Respondenci studenci (różne kierunki)**		**OGÓŁEM**	
Ocena	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***
TAK	500	100%	465	93%	965	96,5%
NIE	0	0%	35	7%	35	3,5%
	500	**100%**	**500**	**100%**	**1000**	**100%**

Źródło: opracowanie własne na podstawie badań własnych

Kadra administracyjna w 100% zadeklarowała, że zachowuje wszystkie zasady ochrony danych osobowych stosowanych w uczelni wyższej przez użytkowników w przypadku korzystania z prywatnego komputera lub laptopa w dostępie do systemów wewnętrznych, zaś studenci tą odpowiedź pozytywnie ocenili w 93%. Znalazły się także osoby, które zadeklarowały, że nie zachowują wszystkich zasad ochrony danych osobowych w dostępie do systemów z prywatnych komputerów i taką odpowiedź zadeklarowało 7%.

Wykres 4.35. odpowiedzi respondentów grupy kadra administracyjna i grupy studenci (różne kierunki) na temat zachowania wszystkich zasad ochrony danych osobowych stosowanych w uczelni wyższej przez użytkowników w przypadku korzystania z prywatnego komputera lub laptopa w dostępie do systemów wewnętrznych



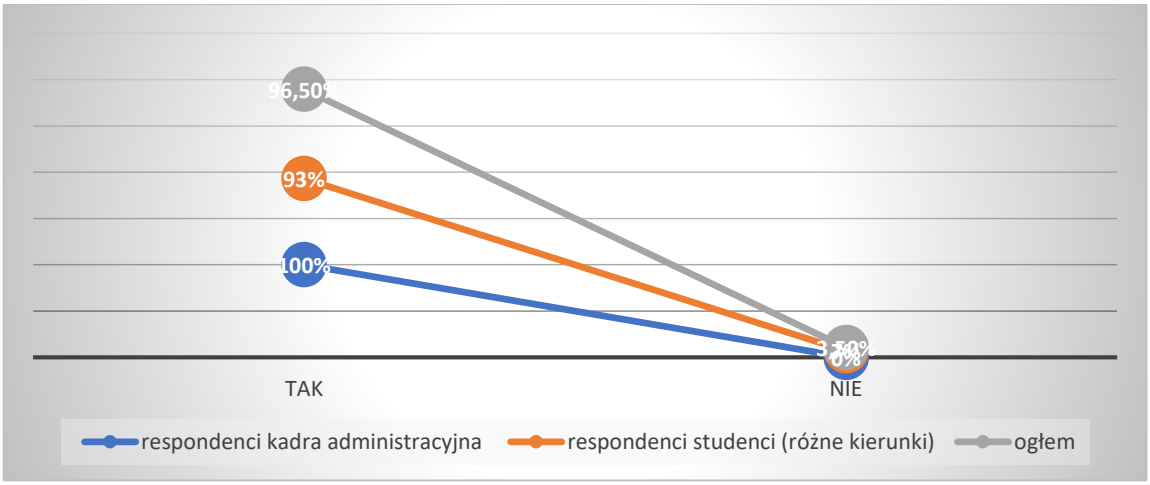
Źródło: opracowanie własne na podstawie badań własnych

Występuje zależność pomiędzy zmiennymi, na co wskazuje współczynnik korelacji liniowej Pearsona na poziomie 1 i współczynnik determinacji liniowej, który prezentuje procent wyjaśnionej liniowo zmienności równy 100%.

$$r_{xy} = \frac{\frac{1}{n}\sum_{i=1}^{n}(x_i-\bar{x})(y_i-\bar{y})}{S_x S_y}=1$$

$$\text{WD}=r_{xy}^{2} * 100\% = 100\%$$

Wykres 4.36. Zależność między respondentami grupy kadra administracyjna i grupy studenci (różne kierunki) pod względem zachowania wszystkich zasad ochrony danych osobowych stosowanych w uczelni wyższej przez użytkowników w przypadku korzystania z prywatnego komputera lub laptopa w dostępie do systemów wewnętrznych



Źródło: opracowanie własne na podstawie badań własnych

Po dokonaniu analizy zależności widać, że wraz ze spadkiem wartości grupy kadry administracyjnej maleją wartości grupy studenci (różne kierunki). Pozwala to wnioskować na bardzo wysoką korelację dodatnią równą 1. W ocenie kadry administracyjnej i studentów wystąpiła deklaracja zachowania zasad ochrony danych podczas korzystania z prywatnych komputerów w dostępie do wewnętrznych systemów.

Należy wyciągnąć wnioski w pytaniu 7 grupy zadeklarowały po 100% i wypowiedziały się pozytywnie na zadane pytanie dotyczące zachowania wszystkich zasad ochrony danych osobowych stosowanych w uczelni wyższej przez użytkowników w przypadku korzystania z prywatnego komputera lub laptopa w dostępie do systemów wewnętrznych. W grupie studentów tą odpowiedź wskazało 93% osób a 7% zaprzeczyło.

Po obserwacji zachowań użytkowników systemu należy stwierdzić, że podobnie jak potwierdzają badania empiryczne pracownicy uczelni wyższych tj. nauczyciele akademiccy i kadra administracyjna starają się zachować większą dyscyplinę korzystając z komputerów prywatnych lub laptopów. Można przypuszczać, że te grupy kierują się większą świadomością wynikających z odmiennych działań konsekwencji. W przypadku studentów taka odpowiedzialność dotycząca naruszeń i świadomość błędów zanika.

Dlatego koncepcja bezpieczeństwa systemu informacyjnego powinna zawierać systematyczne uświadamianie społeczności uczelnianej o obowiązującym prawie ochrony danych osobowych. Uczelnia wyższa ze względu na specyfikę i charakter jest jednostką organizacyjną zatrudniającą pracowników i kształcącą studentów. Występuje w niej ciągła rotacja studentów. Pracownicy zarówno nauczyciele akademiccy jak i kadra administracyjna są to zazwyczaj stanowiska stałe i nie jest zauważalne wzmożenie płynności jak w przypadku studentów.

W badaniach empirycznych ocenie poddano czy użytkownikom zdarza się ujawnić dane innym w przypadku korzystania z prywatnego komputera lub laptopa w dostępie do systemów wewnętrznych.Za pomocą sondażu diagnostycznego w ramach oceny poziomu bezpieczeństwa informacji przez respondentów grupy nauczyciele akademiccy, grupy kadra administracyjna, grupy studenci (różne kierunki), ankietowani mieli możliwość wybrania jednej z dwóch odpowiedzi zaproponowanych „TAK”, lub „NIE”.

8. Czy korzystając z prywatnego komputera/laptopa, w dostępie do systemu informacyjnego zdarza się Państwu ujawnić dane innym osobom do tego nieupoważnionym?

Tabela 4.19. przedstawia rozkład odpowiedzi respondentów grupy nauczyciele akademiccy i grupy kadra administracyjna odpowiadających na pytanie czy korzystając z prywatnego komputera/laptopa, w dostępie do systemu informacyjnego zdarza się Państwu ujawnić dane innym osobom do tego nieupoważnionym?

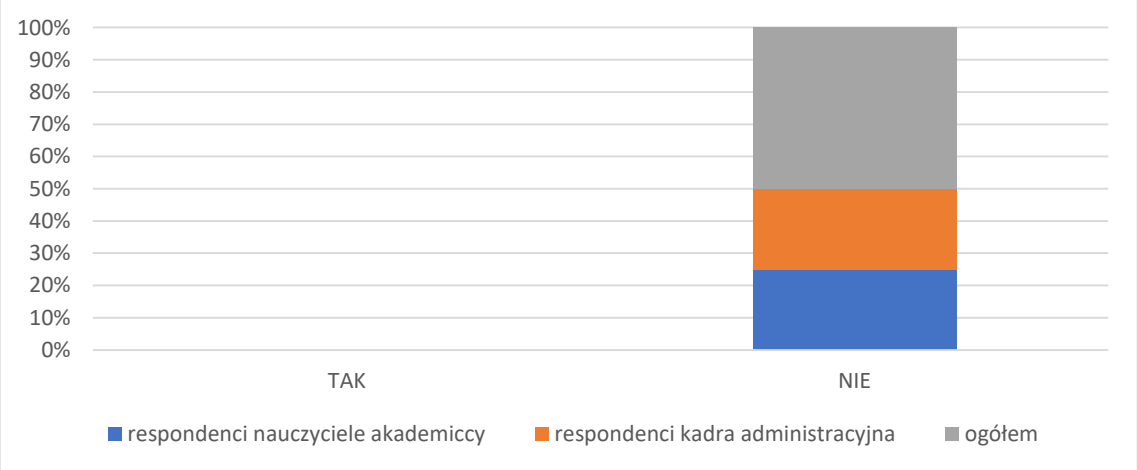
Tabela 4.19. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy kadra administracyjna na temat ujawnienia danych innym osobom w przypadku korzystania z prywatnego komputera/laptopa w dostępie do systemów wewnętrznych uczelni

Odpowiedzi badanych osób Ujawnienie danych osobom nieupoważnionym w przypadku korzystania z prywatnego komputera/laptopa w dostępie do systemów wewnętrznych uczelni						
Osoby poddane badaniu	**Respondenci nauczyciele akademiccy**		**Respondenci kadra administracyjna**		**OGÓŁEM**	
Ocena	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***
TAK	0	0%	0	0%	0	0%
NIE	500	100%	500	100%	1000	100%
	500	**100%**	**500**	**100%**	**1000**	**100%**

Źródło: opracowanie własne na podstawie badań własnych

Ogółem na pytanie 8 odpowiedzi udzieliło 100% respondentów ze wszystkich grup badanych. Nauczyciele akademiccy tak jak i kadra administracyjna zadeklarowały, że nie ujawniają danych innym osobom w przypadku korzystania z prywatnego komputera lub laptopa w dostępie do systemów wewnętrznych uczelni.

Wykres 4.37. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy kadra administracyjna na temat ujawnienia danych osobom nieupoważnionym w przypadku korzystania z prywatnego komputera lub laptopa w dostępie do systemów wewnętrznych uczelni



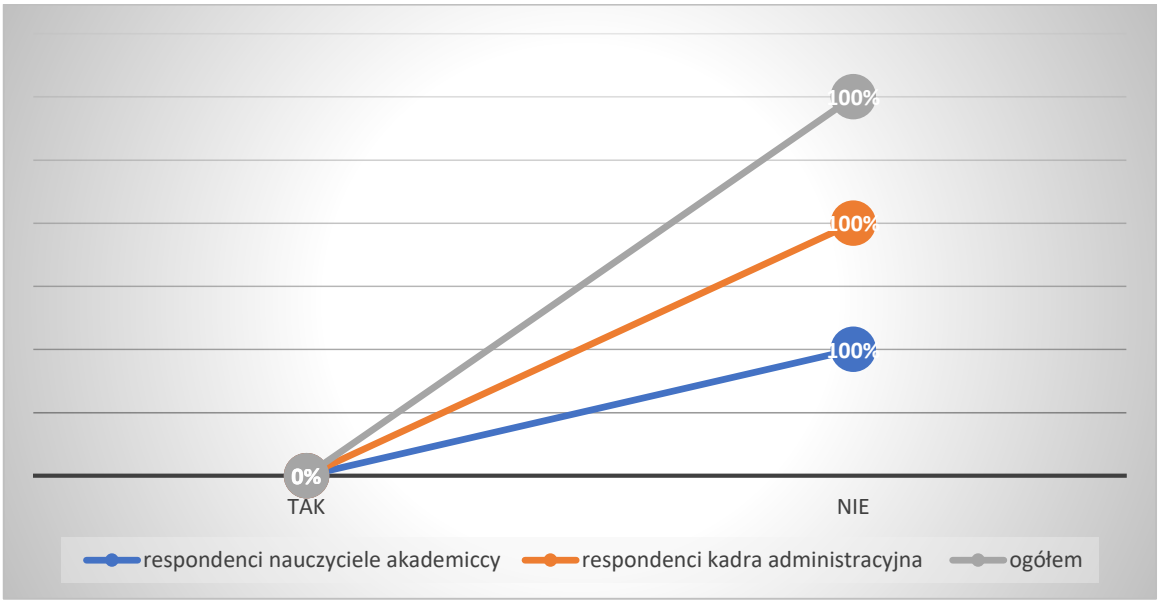
Źródło: opracowanie własne na podstawie badań własnych.

Na zależność między zmiennymi wskazuje współczynnik korelacji liniowej Pearsona na poziomie 1 i współczynnik determinacji liniowej, który przedstawia procent wyjaśnionej liniowo zmienności równy 100%.

$$r_{xy} = \frac{\frac{1}{n}\sum_{i=1}^{n}(x_i-\bar{x})(y_i-\bar{y})}{S_x S_y}=1$$

$$\text{WD}=r_{xy}^{2} * 100\% = 100\%$$

Wykres 4.38. Zależność między respondentami grupy nauczyciele akademiccy i grupy kadra administracyjna pod względem ujawnienia danych osobom nieupoważnionym w przypadku korzystania z prywatnego komputera lub laptopa w dostępie do systemów wewnętrznych uczelni



Źródło: opracowanie własne na podstawie badań własnych

Uogólniając, wraz ze wzrostem wartości wśród nauczycieli akademickich rosną wartości wśród kadry administracyjnej, co oznacza bardzo silną korelację dodatnią. Oznacza to, że w ocenie grupy nauczycieli akademickich i grupy kadra administracyjna nie ujawniają danych logowania do wewnętrznego systemu uczelnianego z prywatnego komputera. W kolejnej tabeli 4.20. zaprezentowano rozkład odpowiedzi dotyczący ujawnienia danych innym w przypadku korzystania z prywatnego komputera lub laptopa w dostępie do systemów wewnętrznych uczelni wśród grupy nauczyciele akademiccy i grupy studenci (różne kierunki).

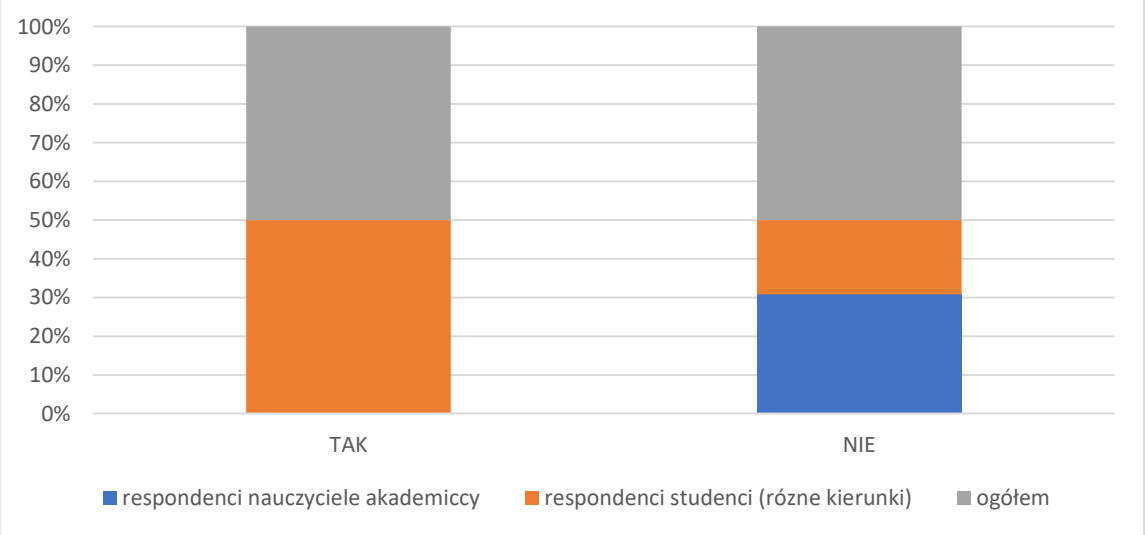
Tabela 4.20. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy studenci (różne kierunki) na temat ujawnienia danych osobom nieupoważnionym w przypadku korzystania z prywatnego komputera lub laptopa w dostępie do systemów wewnętrznych uczelni

Odpowiedzi badanych osób Ujawnienie danych innym osobom w przypadku korzystania z prywatnego komputera/laptopa w dostępie do systemów wewnętrznych uczelni						
Osoby poddane badaniu	**Respondenci nauczyciele akademiccy**		**Respondenci studenci (różne kierunki)**		**OGÓŁEM**	
Ocena	*liczba wskazań*	*udział procentowy*	*liczba wskazań*	*udział procentowy*	*liczba wskazań*	*udział procentowy*
TAK	0	0%	188	37,6%	188	18,8%
NIE	500	100%	312	62,4%	812	81,2%
	500	**100%**	**500**	**100%**	**1000**	**100%**

Źródło: opracowanie własne na podstawie badań własnych

Na temat ujawnienia danych innym osobom w przypadku korzystania z prywatnego komputera lub laptopa w dostępie do systemów wewnętrznych uczelni 312 respondentów. Z grup studentów zadeklarowało, że nie ujawnia takich informacji, co w przeliczeniu procentowym daje 62,4%. Ta sama grupa w ilości 188 respondentów zadeklarowała, że zdarza się ujawnić dane innym osobom, co w przeliczeniu procentowym wynosi 37,6%.

Wykres 225 Wykres 4.39. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy studenci (różne kierunki) na temat ujawnienia danych osobom nieupoważnionym w przypadku korzystania z prywatnego komputera/laptopa w dostępie do systemów wewnętrznych uczelni



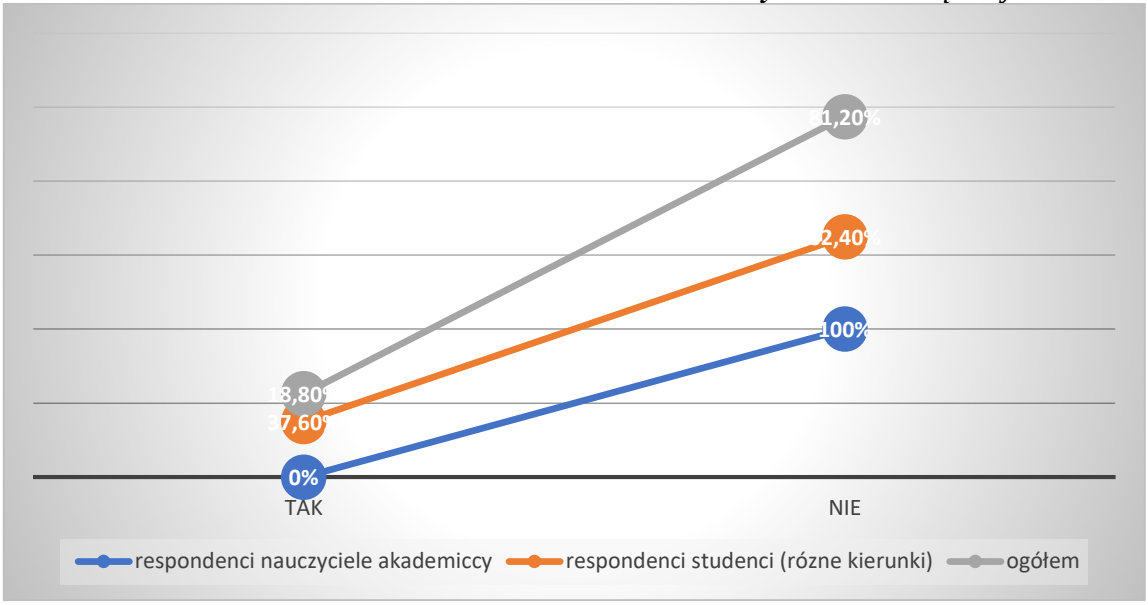
Źródło: opracowanie własne na podstawie badań własnych

Na istnienie zależności wskazuje współczynnik korelacji liniowej Pearsona na poziomie 1 i współczynnik determinacji liniowej, który przedstawia procent wyjaśnionej liniowo zmienności równy 100%.

$$r_{xy} = \frac{\frac{1}{n}\sum_{i=1}^{n}(x_i-\bar{x})(y_i-\bar{y})}{S_x S_y}=1$$

$$\text{WD}=r_{xy}^{2} * 100\% = 100\%$$

Wykres 4.40. Zależność między respondentami grupy nauczyciele akademiccy i grupy studenci (różne kierunki) pod względem ujawnienia danych osobom nieupoważnionym w przypadku korzystania z prywatnego komputera/laptopa w dostępie do systemów wewnętrznych uczelni



Źródło: opracowanie własne na podstawie badań własnych

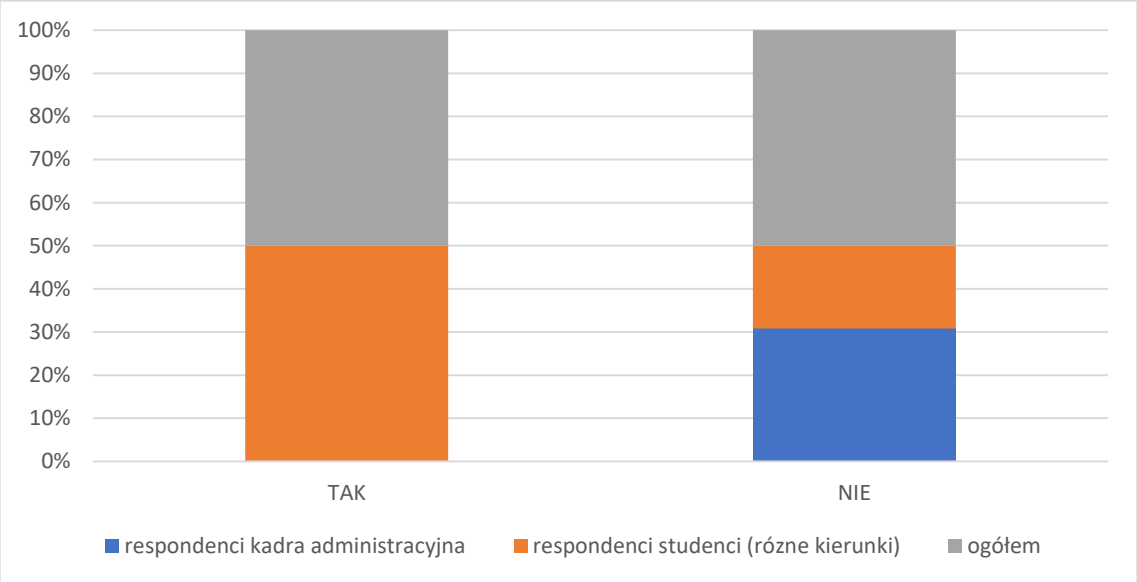
Powyższy rozkład wskazuje, że wraz ze wzrostem wartości wśród nauczycieli akademickich rosną wartości wśród studentów, pozwala to wnioskować na bardzo wysoka korelację dodatnią równą wartości progowej współczynnika korelacji liniowej Pearsona na poziomie 1. W gronie grupy nauczycieli akademickich i grupie studentów nie są ujawniane dane w trakcie użycia prywatnego komputera w dostępie do systemów wewnętrznych uczelni wyższej. Tabela 4.21. przedstawia rozkład odpowiedzi na temat ujawnienia danych innym osobom w przypadku korzystania z prywatnego komputera lub laptopa w dostępie do systemów wewnętrznych uczelni przez grupę kadry administracyjnej i grupę studentów (różnych roczników).

Tabela 4.21. Odpowiedzi respondentów grupy kadra administracyjna i grupy studenci (różne kierunki) na temat ujawnienia danych osobom nieupoważnionym w przypadku korzystania z prywatnego komputera lub laptopa w dostępie do systemów wewnętrznych uczelni

Odpowiedzi badanych osób Ujawnienie danych osobom nieupoważnionym w przypadku korzystania z prywatnego komputera/laptopa w dostępie do systemów wewnętrznych uczelni						
Osoby poddane badaniu	**Respondenci kadra administracyjna**		**Respondenci studenci (różne kierunki)**		**OGÓŁEM**	
Ocena	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***
TAK	0	0%	188	37,6%	188	18,8%
NIE	500	100%	312	62,4%	812	81,2%
	500	**100%**	**500**	**100%**	**1000**	**100%**

Źródło: opracowanie własne na podstawie badań własnych

Wykres 4.41. Odpowiedzi respondentów grupy kadra administracyjna i grupy studenci (różne kierunki) na temat ujawnienia danych osobom nieupoważnionym w przypadku korzystania z prywatnego komputera/laptopa w dostępie do systemów wewnętrznych uczelni



Źródło: opracowanie własne na podstawie badań własnych

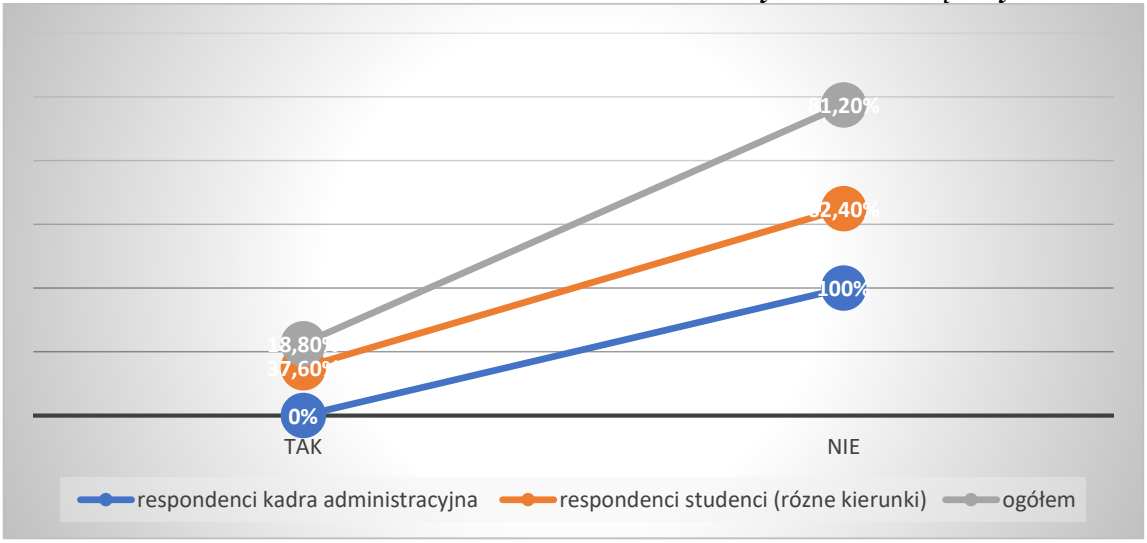
Wśród badanych grup respondentów to nauczyciele akademiccy i kadra administracyjna w 100% zadeklarowały, że nie ujawniają danych innym osobom w przypadku korzystania z systemów wewnętrznych na prywatnym komputerze lub laptopie w dostępie do systemów wewnętrznych w uczelni wyższej. Studenci zadeklarowali nieujawnianie danych osobom nieuprawnionym w przypadku korzystania z prywatnego komputera/laptopa w dostępie do systemów wewnętrznych uczelni w ilości 62,4%.

Jeżeli chodzi o zależność to świadczy o niej współczynnik korelacji liniowej Pearsona na poziomie 1 i współczynnik determinacji liniowej, który wskazuje procent wyjaśnionej liniowo zmienności i jest równy 100%.

$$r_{xy} = \frac{\frac{1}{n}\sum_{i=1}^{n}(x_i-\bar{x})(y_i-\bar{y})}{S_x S_y}=1$$

$$\text{WD}=r_{xy}^{2} * 100\% = 100\%$$

Wykres 4.42. Zależność między respondentami grupy kadra administracyjna i grupy studenci (różne kierunki)) pod względem ujawnienia danych osobom nieupoważnionym w przypadku korzystania z prywatnego komputera/laptopa w dostępie do systemów wewnętrznych uczelni



Źródło: opracowanie własne na podstawie badań własnych

Dokonując analizy zależności jednej i drugiej badanej grupy widać, że wraz ze wzrostem pierwszej grupy respondentów, jakimi są kadra administracyjna rosną wartości drugiej grupy studentów (różnych kierunków). Fakt ten pozwala wnioskować na bardzo silną korelację dodatnią równą wartości progowej współczynnika korelacji liniowej Pearsona na poziomie 1. Kadra administracyjna jak i studenci deklarują, że nie ujawniają danych innym osobom podczas użycia prywatnego komputera lub laptopa w dostępie do systemów wewnętrznych uczelni wyższej.

Uogólniając, należy zaznaczyć, że takie grupy jak nauczyciele akademiccy i kadra administracyjna jednomyślnie zaopiniowały zachowanie standardów nie ujawniania danych innym osobom podczas korzystania z komputera lub laptopa z prywatnego konta. W grupie studentów pojawiły się jednostki, które zadeklarowały, że takich jak powyżej wspomniane działania nie są przez nich praktykowane.

Opierając swoje spostrzeżenia i końcowy wniosek oraz mając na uwadze opinię eksperta, osób przestrzegających pewne wdrożone zasady jest zauważalnie dużo. Niemniej widoczne jest także pojawienie się wśród dwóch grup, jakimi są nauczyciele akademiccy i kadra administracyjna poprawności służbowej, która nie pozwoliła na udzielenie prawdziwej odpowiedzi. Podstawą przypuszczeń jest fakt, że korzystając z komputerów czy laptopów w zaciszu domowym są także domownicy, którzy najczęściej mają wgląd w przeglądane dane. Urządzenia przenośne takie jak laptopy często są wykorzystywane w przestrzeni publicznej to także jest strefa gdzie osoby postronne mają możliwość podglądu wyświetlonych danych.

W koncepcji zmian należy zaproponować szkolenia dla wszystkich grup użytkowników systemu wewnętrznego uczelni wyższej z zakresu ochrony informacji, bezpieczeństwa systemów informacyjnych. Będzie to miało na celu propagowanie kultury pracy z systemem oraz zwiększy społeczną świadomość i uświadomi uczestnikom o ryzykownym zachowaniu wykorzystując i udostępniając dane. W badaniach empirycznych ocenie poddano ***czy użytkownicy po zalogowaniu się na swoje konto zapoznali się z instrukcjami dostępnymi w szczególności zasadami korzystania z systemu?*** Za pomocą sondażu diagnostycznego w ramach oceny bezpieczeństwa informacji przez respondentów grupy nauczyciele akademiccy, kadra administracyjna, grupy studenci (różne kierunki) ankietowani mieli możliwość udzielenia jednej z dwóch proponowanych odpowiedzi „TAK", lub „NIE".

9. Czy korzystacie Państwo podczas logowania z dostępnymi instrukcjami ułatwiającymi korzystanie z systemu informacyjnego?

Rozkład odpowiedzi na powyższe pytanie został uwzględniony w tabeli 4.22 gdzie odpowiedzi udzielały dwie grupy, nauczyciele akademiccy i kadra administracyjna.

Tabela 4.22. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy kadra administracyjna na temat zapoznania się przez nich z dostępnymi instrukcjami ułatwiającymi korzystanie z systemu informacyjnego w uczelni wyższej

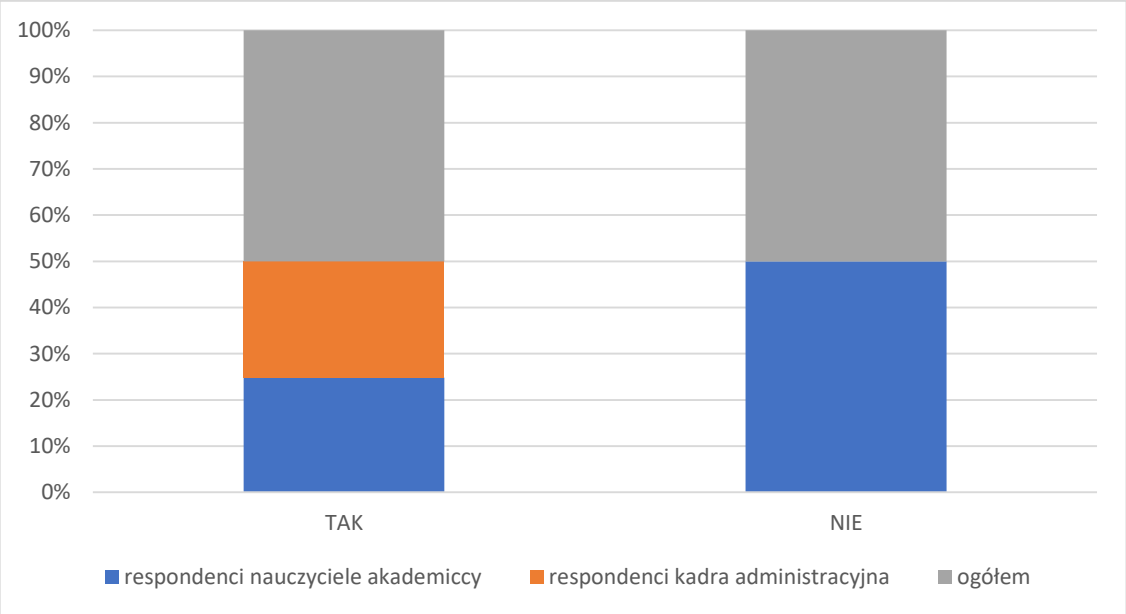
Odpowiedzi badanych osób *zapoznania się przez nich z dostępnymi instrukcjami ułatwiającymi korzystanie z systemu informacyjnego w uczelni wyższej*						
Osoby poddane badaniu	**Respondenci nauczyciele akademiccy**		**Respondenci kadra administracyjna**		**OGÓŁEM**	
Ocena	*liczba wskazań*	*udział procentowy*	*liczba wskazań*	*udział procentowy*	*liczba wskazań*	*udział procentowy*
TAK	492	98,4%	500	100%	992	99,2%

NIE	8	1,6%	0	0%	8	0,8%
	500	**100%**	**500**	**100%**	**1000**	**100%**

Źródło: opracowanie własne na podstawie badań własnych

Z oceny uzyskanych wyników badań wynika, że 492 respondentów, co w przeliczeniu procentowym wynosi 98,4% deklaruje zapoznanie się z instrukcjami dostępnymi w szczególności z zasadami korzystania z systemu uczelni wyższej. Brak zapoznania z instrukcjami tą odpowiedź w powyższej grupie zadeklarowało 8 osób, co w przeliczeniu procentowym wynosi 1,6%. Kadra administracyjna zadeklarowała w 100% zapoznanie się z instrukcjami i zasadami korzystania z systemu uczelni wyższej.

Wykres 4.43. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy kadra administracyjna na temat zapoznania się przez nich z dostępnymi instrukcjami ułatwiającymi korzystanie z systemu informacyjnego w uczelni wyższej



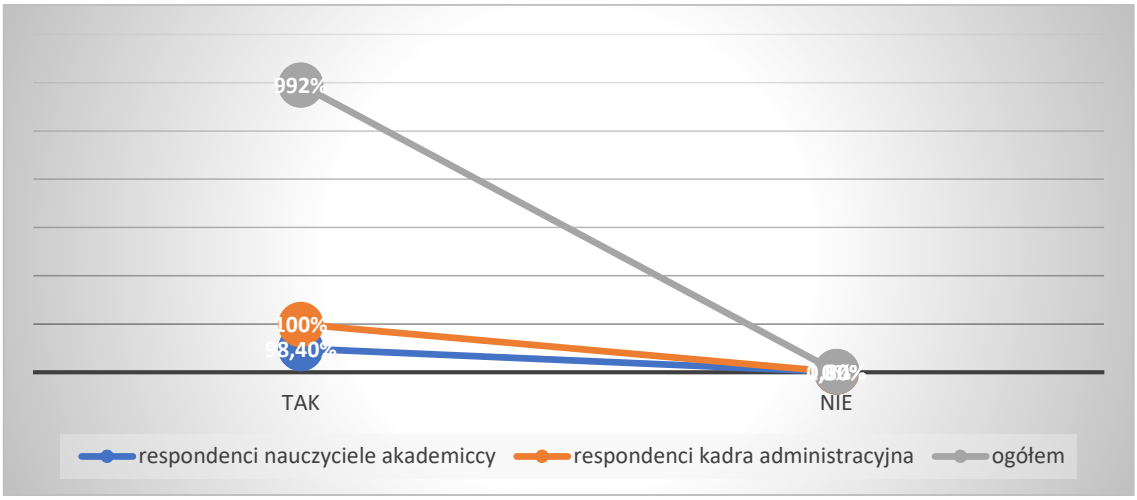
Źródło: opracowanie własne na podstawie badań własnych

Na zależność między grupą nauczycieli akademickich i grupą kadry administracyjnej wskazuje współczynnik korelacji liniowej Pearsona kształtujący się na poziomie 1 i współczynnik determinacji liniowej, który przedstawia procent wyjaśnionej liniowo zmienności równy 100%.

$$r_{xy} = \frac{\frac{1}{n}\sum_{i=1}^{n}(x_i-\bar{x})(y_i-\bar{y})}{S_x S_y}=1$$

$$\mathrm{WD}=r_{xy}^{2} * 100\% = 100\%$$

Wykres 4.44. Zależność między grupą nauczyciele akademiccy i grupą kadra administracyjna pod zapoznania się przez nich z dostępnymi instrukcjami ułatwiającymi korzystanie z systemu informacyjnego w uczelni wyższej



Źródło: opracowanie własne na podstawie badań własnych

Powyższy rozkład wskazuje, że wraz ze spadkiem wartości wśród nauczycieli akademickich maleją wartości wśród kadry administracyjnej, co wskazuje na bardzo silną korelację dodatnią równą wartości progowej współczynnika korelacji liniowej Pearsona na poziomie 1. W opinii jednej i drugiej grupy zapoznano się z instrukcjami. Rozkład odpowiedzi na powyższe pytanie został uwzględniony w tabeli 4.23 gdzie odpowiedzi udzielały dwie grupy, nauczyciele akademiccy i studenci (różne kierunki).

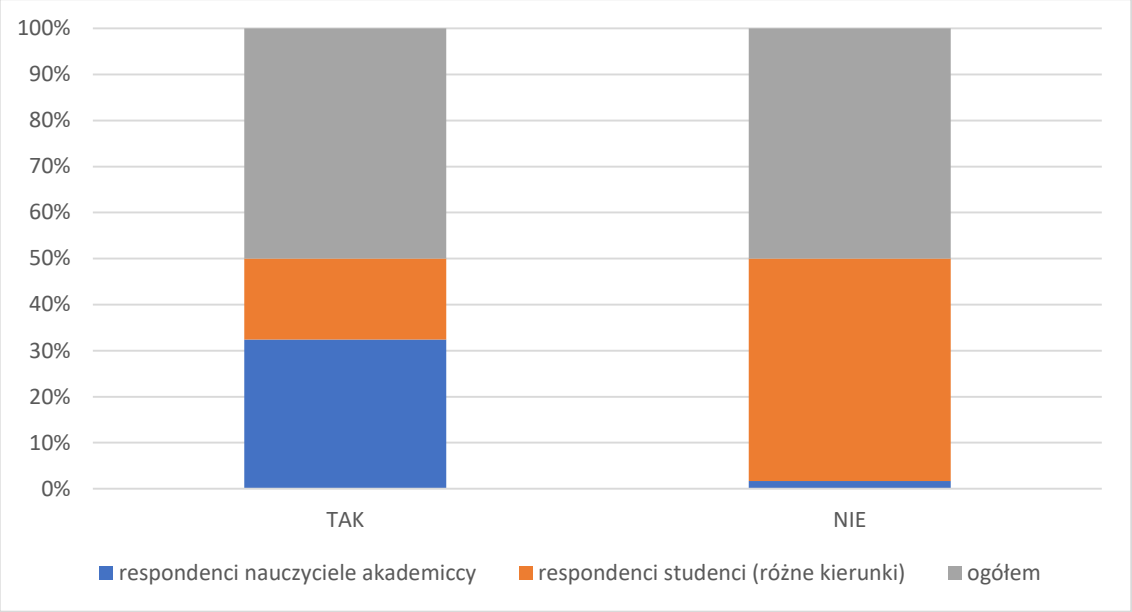
Tabela 4.23. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy studenci (różne kierunki) na temat zapoznania się przez nich z dostępnymi instrukcjami ułatwiającymi korzystanie z systemu informacyjnego w uczelni wyższej

Odpowiedzi badanych osób *zapoznania się przez nich z dostępnymi instrukcjami ułatwiającymi korzystanie z systemu informacyjnego w uczelni wyższej*						
Osoby poddane badaniu	**Respondenci nauczyciele akademiccy**		**Respondenci studenci (różne kierunki)**		**OGÓŁEM**	
Ocena	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***
TAK	492	98,4%	267	53,4%	759	75,9%
NIE	8	1,6%	233	46,6%	241	24,1%
	500	**100%**	**500**	**100%**	**1000**	**100%**

Źródło: opracowanie własne na podstawie badań własnych

Z oceny uzyskanych wyników badań wynika, że 267 respondentów z grupy studentów zadeklarowało zapoznanie się przez nich z instrukcjami dostępnymi w szczególności z zasadami korzystania z systemu uczelni wyższej, co w przeliczeniu procentowym wynosi 53,4%. Odmienną odpowiedź w tej grupie zadeklarowało 233 osoby, co w przeliczeniu procentowym daje 46,6%.

Wykres 4.45. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy studenci (różne kierunki) na temat zapoznania się przez nich z dostępnymi instrukcjami ułatwiającymi korzystanie z systemu informacyjnego w uczelni wyższej



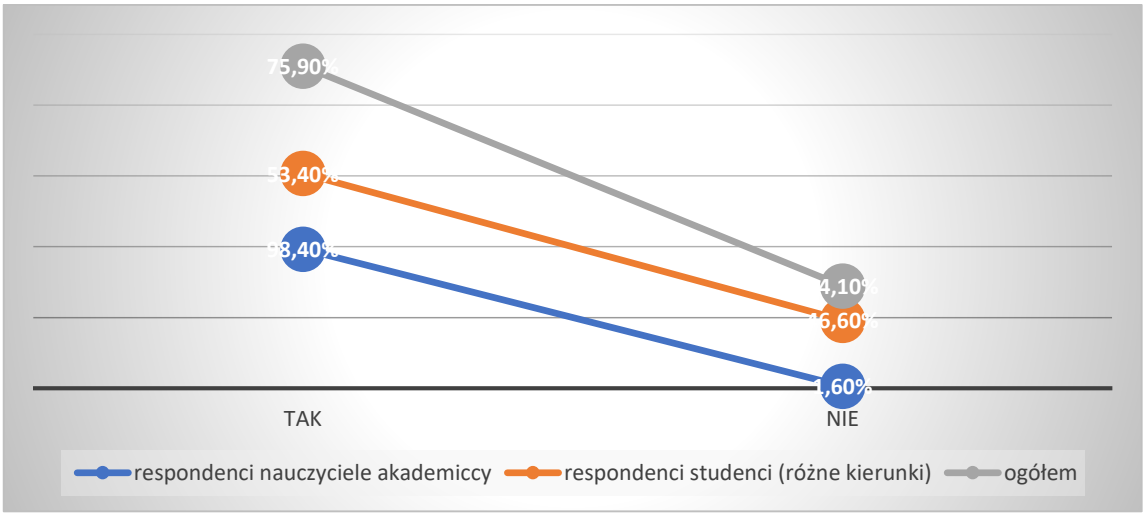
Źródło: opracowanie własne na podstawie badań własnych

Na zależność pomiędzy respondentami grupy nauczyciele akademiccy i grupy studenci (różnych kierunków) wskazuje współczynnik korelacji liniowej Pearsona na poziomie 1 i współczynnik determinacji liniowej, który przedstawia procent wyjaśnionej liniowo zmienności równy 100%.

$$r_{xy} = \frac{\frac{1}{n}\sum_{i=1}^{n}(x_i-\bar{x})(y_i-\bar{y})}{S_x S_y}=1$$

$$\mathrm{WD}=r_{xy}^{2} * 100\% = 100\%$$

Wykres 4.46. Zależność między grupą nauczyciele akademiccy i studenci (różne kierunki) pod względem zapoznania się przez nich z dostępnymi instrukcjami ułatwiającymi korzystanie z systemu informacyjnego w uczelni wyższej



Źródło: opracowanie własne na podstawie badań własnych

Powyższy rozkład wskazuje, że wraz ze spadkiem wartości wśród nauczycieli akademickich, wartości deklarowane przez grupę studentów także maleją. W opinii nauczycieli i studentów zapoznano się z instrukcjami dostępnymi w szczególności z zasadami korzystania z systemu uczelni wyższej. Rozkład odpowiedzi na powyższe pytanie został uwzględniony w tabeli 4.24 gdzie odpowiedzi udzielały dwie grupy, kadra administracyjna i studenci (różne kierunki).

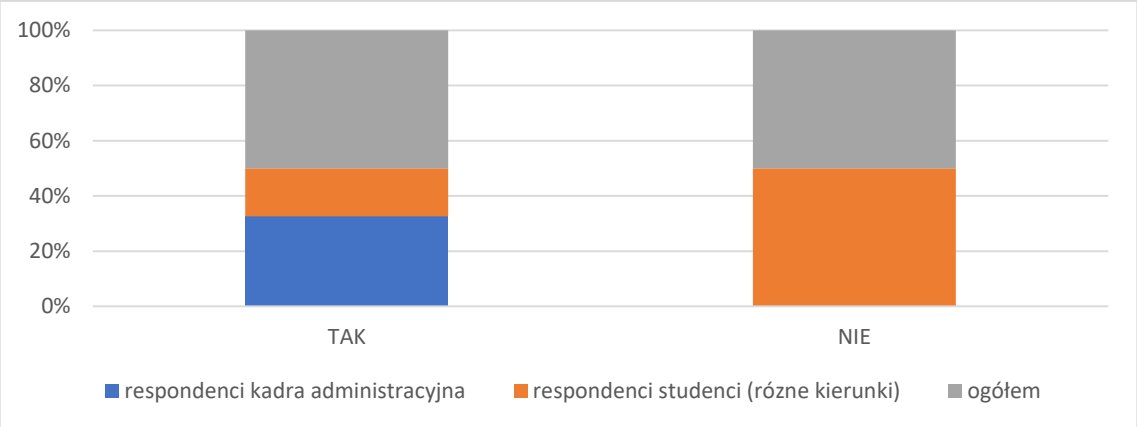
Tabela 4.24. Odpowiedzi respondentów grupy kadra administracyjna i grupy studenci (różne kierunki) na temat zapoznania się przez nich z dostępnymi instrukcjami ułatwiającymi korzystanie z systemu informacyjnego w uczelni wyższej

Odpowiedzi badanych osób *zapoznania się przez nich z dostępnymi instrukcjami ułatwiającymi korzystanie z systemu informacyjnego w uczelni wyższej*						
Osoby poddane badaniu	**Respondenci kadra administracyjna**		**Respondenci studenci (różne kierunki)**		**OGÓŁEM**	
Ocena	*liczba wskazań*	*udział procentowy*	*liczba wskazań*	*udział procentowy*	*liczba wskazań*	*udział procentowy*
TAK	500	100%	267	53,4%	767	76,7%
NIE	0	0%	233	46,6%	233	23,3%
	500	**100%**	**500**	**100%**	**1000**	**100%**

Źródło: opracowanie własne na podstawie badań własnych

Poddając pod analizę wyniki badań widać, że kadra administracyjna w 100% deklaruje zapoznanie się z instrukcjami, zaś studenci tylko w 53,4%.

Wykres 4.47. Odpowiedzi respondentów grupy kadra administracyjna i grupy studenci (różne kierunki) na temat zapoznania się przez nich z dostępnymi instrukcjami ułatwiającymi korzystanie z systemu informacyjnego w uczelni wyższej



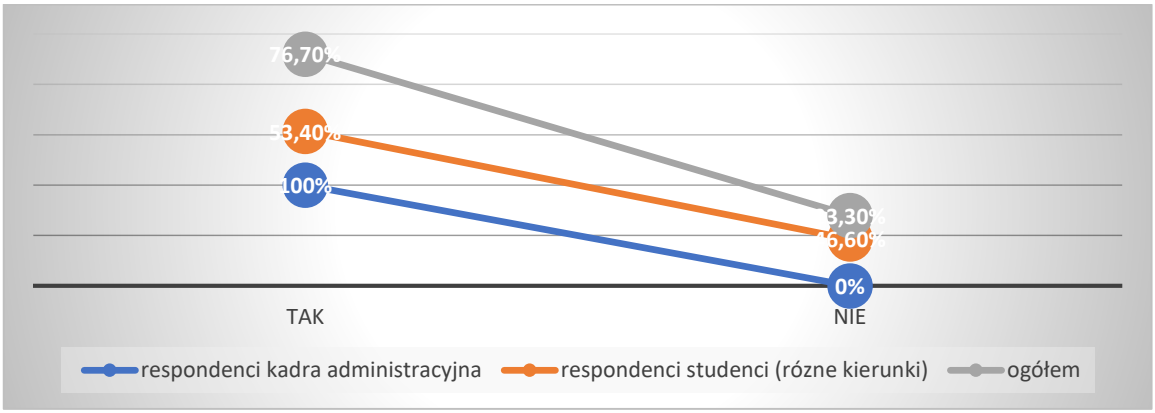
Źródło opracowanie własne na podstawie badań własnych

Na zależność pomiędzy respondentami grupy kadra administracyjna i grupy studenci (różnych kierunków) wskazuje współczynnik korelacji liniowej Pearsona na poziomie 1 i współczynnik determinacji liniowej, który przedstawia procent wyjaśnionej liniowo zmienności równy 100%.

$$r_{xy} = \frac{\frac{1}{n}\sum_{i=1}^{n}(x_i-\bar{x})(y_i-\bar{y})}{S_x S_y}=1$$

$$\mathrm{WD}=r_{xy}^{2} * 100\% = 100\%$$

Wykres 4.48. Zależność między grupą kadra administracyjna i studenci (różne kierunki) pod względem zapoznania się przez nich z dostępnymi instrukcjami ułatwiającymi korzystanie z systemu informacyjnego w uczelni wyższej



Źródło: opracowanie własne na podstawie badań własnych

Dokonując analizy zależności wraz ze spadkiem wartości wśród kadry administracyjnej maleją wartości wśród studentów (różnych kierunków), pozwala to wnioskować na bardzo silną korelację dodatnią równą wartości progowej współczynnika korelacji

liniowej Pearsona na poziomie 1. Wartości pozyskane świadczą o tym, że kadra administracyjna i studenci zapoznają się z instrukcjami.

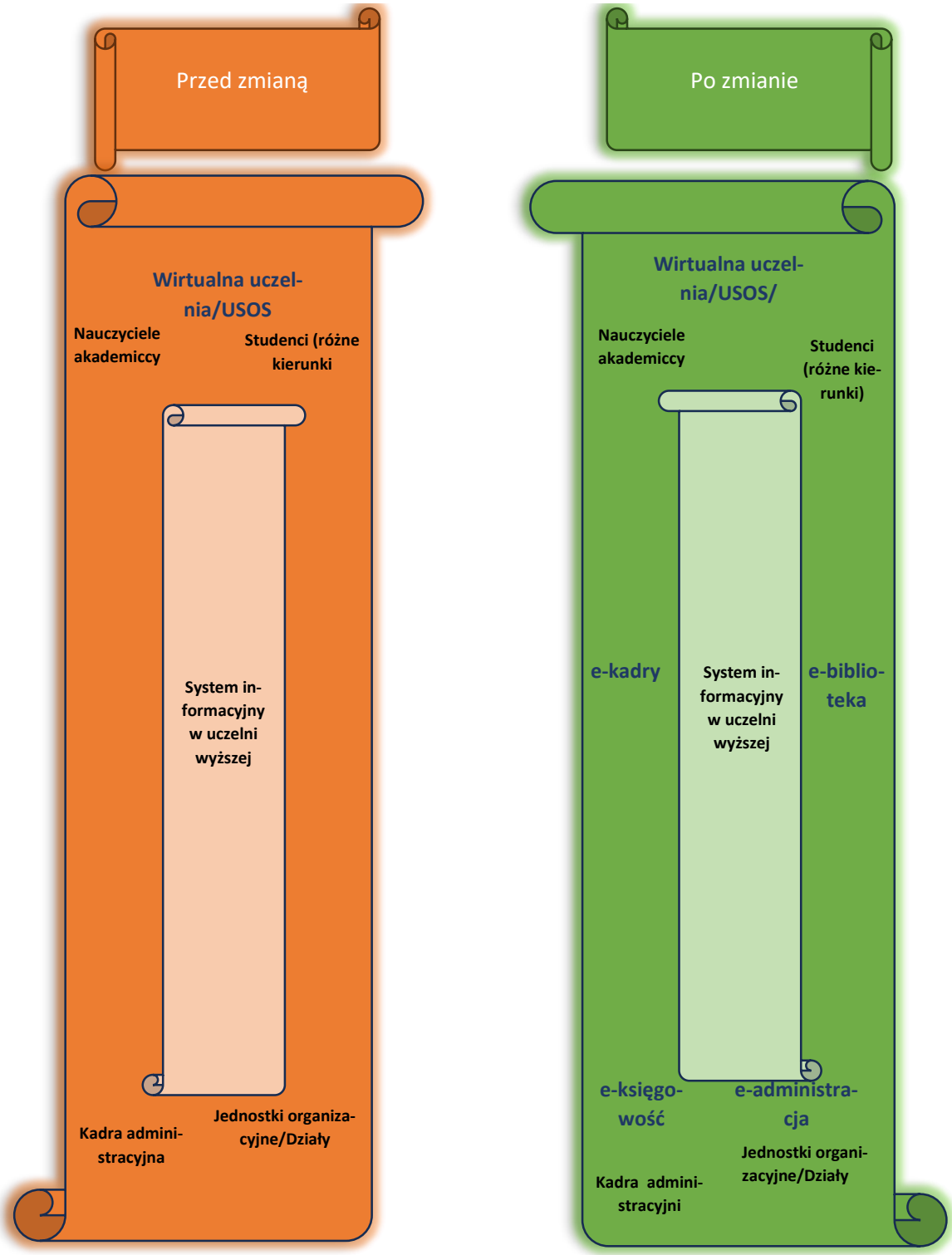
Wnioskując po analizie danych widać, iż nie wszyscy respondenci deklarują, że zapoznali się z instrukcjami dostępnymi w szczególności z zasadami korzystania z sytemu uczelni wyższej. Praktyka jednak pokazuje, że takie instrukcje często są pomijane przez użytkowników, ponieważ zwykle jest na nich dużo treści. W opinii użytkowników są uznawane za mało interesujące i czas na ich przeczytanie jest długi, są one nudne i zawierają standardowe i powtarzalne przekazy niestanowiące w opinii użytkowników żadnej podstawowej wartości.

Powyższa analiza wskazuje, że kolejny raz pojawia się brak prawdziwości i autentyczności udzielania odpowiedzi na pytanie. Dlatego też w koncepcji bezpieczeństwa systemu informacyjnego w uczelni wyższej powinno się odejść od tego rodzaju form a w zamian powinien pojawić się krótki spot instruktażowy, który pobudzi wyobraźnię użytkowników korzystających z systemu informacyjnego. Powyższy proponowany spot powinien zawierać treści merytoryczne, konkretne, przedstawione za pomocą obrazu i dźwięku a w takiej wersji jest szybciej zapamiętany. Powinien być lektor posiadający odpowiednią tonację głosu (treści przekazywana nie za szybko, nie za wolno), prosty komunikat z łatwo przyswajalnymi informacjami. Taki proces pozwoli na spełnienie oczekiwań ówczesnego społeczeństwa opierającego się na takich przekazach. Rysunek 4.51. przedstawia zintegrowany system informacyjny przed i po zmianie.

Z literatury podanej analizie wynika, że tyko 10 % informacji przeczytanej zapamiętuje mózg człowieka w przypadku obrazu jest to aż 50%, dlatego taka informacja podtrzymuje prawidłowość wprowadzenia multimedialnego filmiku.

W badaniach empirycznych ocenie poddano czy użytkownicy korzystają z konta indywidualnego systemu informacyjnego w uczelni wyższej i z jaka częstotliwością. Za pomocą sondażu diagnostycznego w ramach oceny częstotliwości korzystania z konta systemu informacyjnego, respondenci grupy nauczyciele akademiccy, kadra administracyjna i studenci (różne kierunki) mieli możliwość udzielenia jednej z dwóch proponowanych odpowiedzi „TAK” ze wskazaniem częstotliwości lub „NIE”.

Rysunek 4.3.Zintegrowany system przed i po zmianie



Źródło: opracowanie własne

10. Czy korzystacie Państwo z konta indywidualnego, systemu informatycznego założonego każdemu pracownikowi uczelni/studentowi uczelni? Rozkład odpowiedzi respondentów prezentuje tabela 4.25.

Tabela 4.25. Odpowiedzi respondentów grupy nauczyciele akademiccy, grupy kadra administracyjna na temat korzystania z konta indywidualnego, systemu informatycznego założonego każdemu pracownikowi uczelni/studentowi uczelni

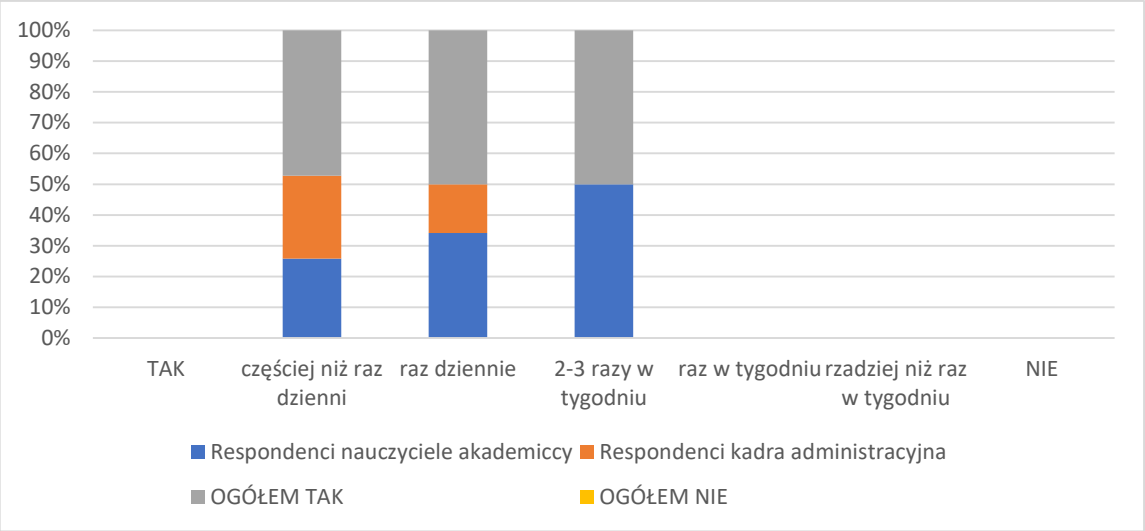
Odpowiedzi badanych osób *Korzystanie z konta indywidualnego, systemu informatycznego założonego każdemu pracownikowi w uczelni wyższej*						
Odpowiedź	**Respondenci nauczyciele akademiccy**		**Respondenci kadra administracyjna**		**OGÓŁEM**	
TAK	*liczba wskazań*	*udział procentowy*	*liczba wskazań*	*udział procentowy*	*liczba wskazań*	*udział procentowy*
częściej niż raz dzienni	467	93,4%	487	97,4%	854	85,4%
raz dziennie	28	5,6%	13	2,6%	41	4,1%
2-3 razy w tygodniu	5	1%	0	0%	5	0,5%
raz w tygodniu	0	0%	0	0%	0	0%
rzadziej niż raz w tygodniu	0	0%	0	0%	0	0%
NIE	0	0%	0	0%	0	0%
	500	**100%**	**500**	**100%**	**1000**	**100%**

Źródło: Opracowanie własne na podstawie badań własnych

Odpowiedzi na powyższe pytanie udzieliło 100% respondentów. Z odpowiedzi badanych osób wynika, że aż 93,4% respondentów z grupy nauczycieli akademickich i 97,4% z grupy kadry administracyjnej deklaruje, że korzysta z konta indywidualnego częściej niż raz dziennie.

Nikt z powyższych respondentów nie zadeklarował korzystania z konta rzadziej niż raz w tygodniu. Wszyscy respondenci zadeklarowali, korzystanie z kont indywidualnych.

Wykres 4.49. Odpowiedzi respondentów grupy nauczyciele akademiccy, grupy kadra administracyjna na temat korzystania z konta indywidualnego, systemu informatycznego założonego każdemu pracownikowi uczelni/studentowi uczelni



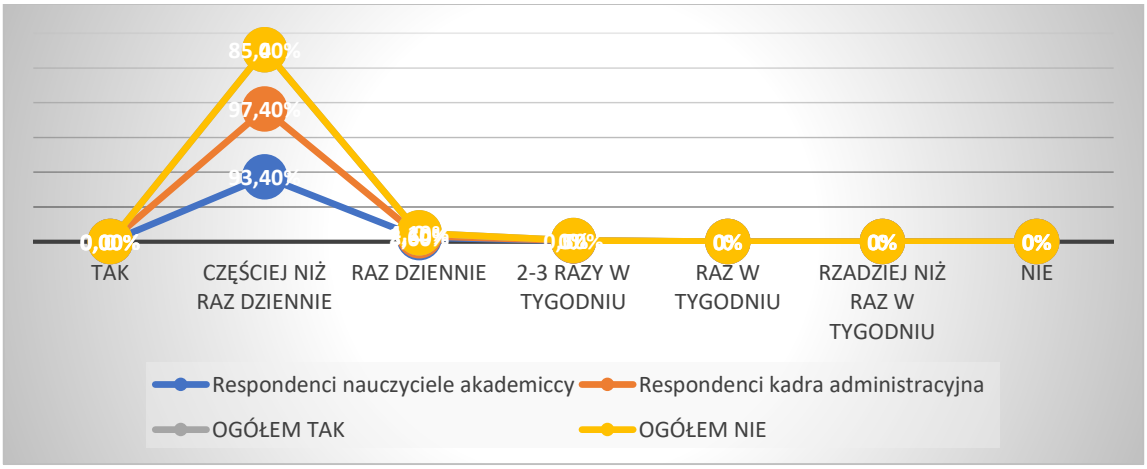
Źródło: Opracowanie własne na podstawie badań własnych

Istnieje zależność, o której świadczy współczynnik korelacji liniowej Pearsona będący na poziomie 1 i współczynnik determinacji liniowej, który wskazuje procent wyjaśnionej liniowo zmienności równy 100%.

$$r_{xy} = \frac{\frac{1}{n}\sum_{i=1}^{n}(x_i-\bar{x})(y_i-\bar{y})}{S_x S_y}=1$$

$$\mathrm{WD}=r_{xy}^{2} * 100\% = 100\%$$

Wykres 4.50.Zależnosci pomiędzy respondentami grupy nauczyciele akademiccy, grupy kadra administracyjna na temat korzystania z konta indywidualnego, systemu informatycznego założonego każdemu pracownikowi uczelni/studentowi uczelni



Źródło: Opracowanie własne na podstawie badań własnych

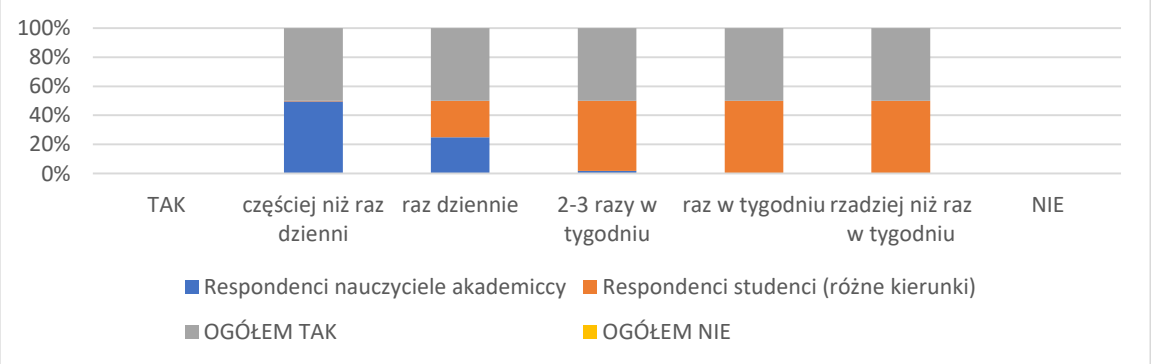
Tabela 4.26. Odpowiedzi respondentów grupy nauczyciele akademiccy, grupy studenci (różne kierunki) na temat korzystania z konta indywidualnego, systemu informatycznego założonego każdemu pracownikowi uczelni/studentowi uczelni

Odpowiedzi badanych osób *Korzystanie z konta indywidualnego, systemu informatycznego założonego każdemu pracownikowi w uczelni wyższej*						
Odpowiedź	**Respondenci nauczyciele akademiccy**		**Respondenci studenci (różne kierunki)**		**OGÓŁEM**	
TAK	*liczba wskazań*	*udział procentowy*	*liczba wskazań*	*udział procentowy*	*liczba wskazań*	*udział procentowy*
częściej niż raz dzienni	467	93,4%	4	0,8%	471	47,1%
raz dziennie	28	5,6%	28	5,6%	56	5,6%
2-3 razy w tygodniu	5	1%	128	25,6%	133	13,3%
raz w tygodniu	0	0%	186	37,2%	186	18,6%
rzadziej niż raz w tygodniu	0	0%	154	30,8%	154	15,4%
NIE	0	0%	0	0%	0	0%
	500	**100%**	**500**	**100%**	**1000**	**100%**

Źródło: Opracowanie własne na podstawie badań własnych

Pozyskane odpowiedzi pokazały, że studenci rzadziej korzystają z kont utworzonych przez uczelnię. W przypadku tej grupy respondentów odpowiedzią najczęściej typowaną była „raz w tygodniu". To właśnie tą odpowiedź zadeklarowało 37,2% respondentów w badanej grupie.

Wykres 4.51. Odpowiedzi respondentów grupy nauczyciele akademiccy, grupy studenci (różne kierunki) na temat korzystania z konta indywidualnego, systemu informatycznego założonego każdemu pracownikowi uczelni/studentowi uczelni



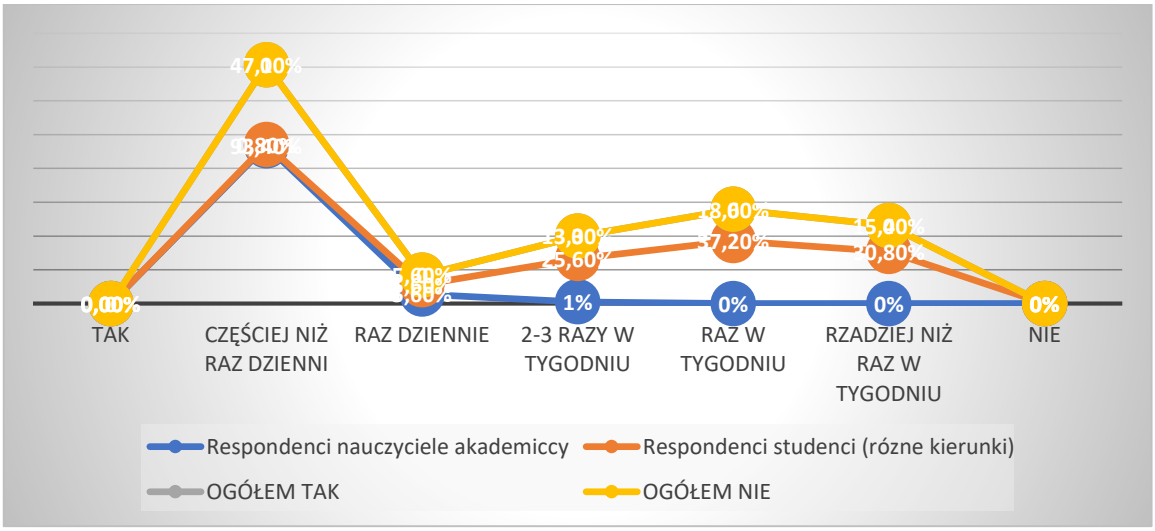
Źródło: Opracowanie własne na podstawie badań własnych

Z oceny uzyskanych wyników na temat częstotliwości korzystania z kont indywidualnych systemu informatycznego założonego każdemu pracownikowi/studentowi wynika zależność, ·o czym świadczy współczynnik korelacji liniowej Pearsona na poziomie – 0,71 i współczynnik determinacji liniowej 50,41%.

$$r_{xy} = \frac{\frac{1}{n}\sum_{i=1}^{n}(x_i-\bar{x})(y_i-\bar{y})}{S_x S_y}\text{=-0,71}$$

$$\text{WD=r}\frac{2}{xy} * 100\% = 50{,}41\%$$

Wykres 4.52. Zależności pomiędzy respondentami grupy nauczyciele akademiccy, grupy studenci (różne kierunki) na temat korzystania z konta indywidualnego, systemu informatycznego założonego każdemu pracownikowi uczelni/studentowi uczelni



Źródło: Opracowanie własne na podstawie badań własnych

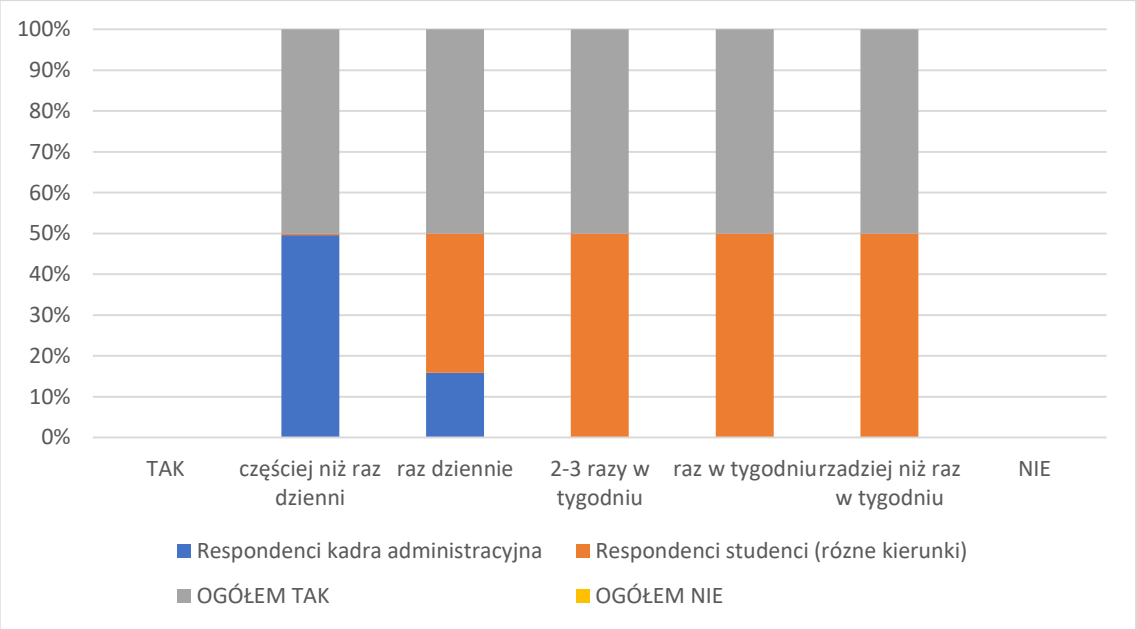
Tabela 4.27. Odpowiedzi respondentów grupy kadra administracyjna, grupy studenci (różne kierunki) na temat korzystania z konta indywidualnego, systemu informatycznego założonego każdemu pracownikowi uczelni/studentowi uczelni

Odpowiedzi badanych osób ***Korzystanie z konta indywidualnego, systemu informatycznego założonego każdemu pracownikowi w uczelni wyższej***						
Odpowiedź	**Respondenci kadra administracyjna**		**Respondenci studenci (różne kierunki)**		**OGÓŁEM**	
TAK	*liczba wskazań*	*udział procentowy*	*liczba wskazań*	*udział procentowy*	*liczba wskazań*	*udział procentowy*
częściej niż raz dzienni	487	97,4%	4	0,8%	491	49,1%
raz dziennie	13	2,6%	28	5,6%	41	4,1%

2-3 razy w tygodniu	0	0%	128	25,6%	128	12,8%
raz w tygodniu	0	0%	186	37,2%	186	18,6%
rzadziej niż raz w tygodniu	0	0%	154	30,8%	154	15,4%
NIE	0	0%	0	0%	0	0%
	500	**100%**	**500**	**100%**	**1000**	**100%**

Źródło: Opracowanie własne na podstawie badań własnych

Wykres 4.53. Odpowiedzi respondentów grupy kadra administracyjna, grupy studenci (różne kierunki) na temat korzystania z konta indywidualnego, systemu informatycznego założonego każdemu pracownikowi uczelni/studentowi uczelni



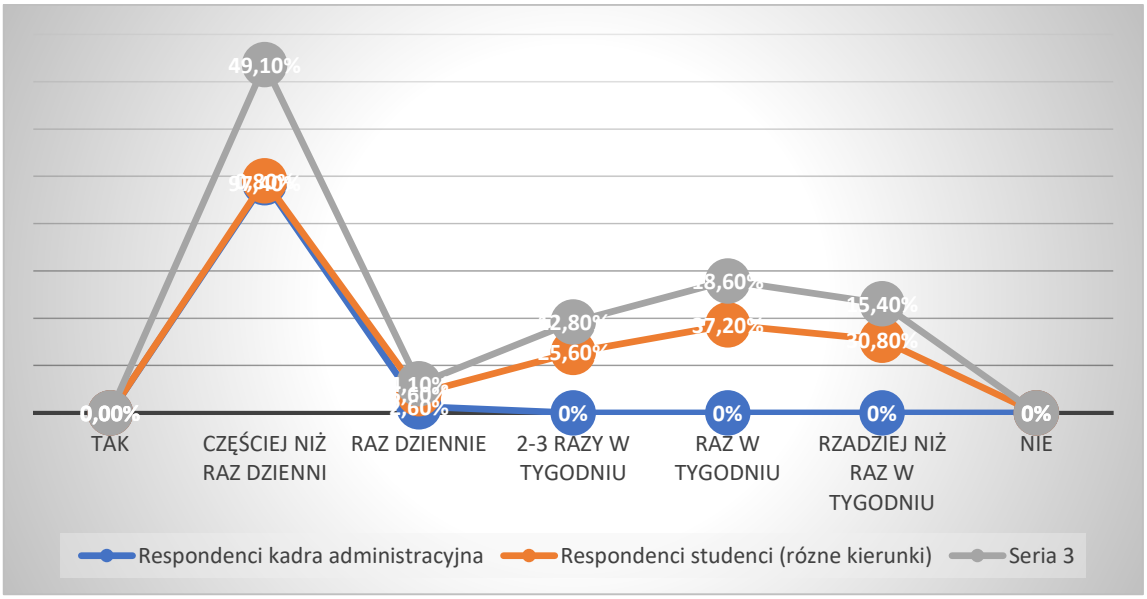
Źródło: Opracowanie własne na podstawie badań własnych

Z badań wynika współzależność pomiędzy grupami, o czym świadczy współczynnik korelacji liniowej Pearsona na poziomie -0,69 i współczynnik determinacji liniowej na poziomie 47,61%.

$$r_{xy} = \frac{\frac{1}{n}\sum_{i=1}^{n}(x_i-\bar{x})(y_i-\bar{y})}{S_x S_y} = -0{,}69$$

$$\mathrm{WD} = r_{xy}^2 * 100\% = 47{,}61\%$$

Wykres 4.54. Zależności pomiędzy respondentami grupy kadra administracyjna, grupy studenci (różne kierunki) na temat korzystania z konta indywidualnego, systemu informatycznego założonego każdemu pracownikowi uczelni/studentowi uczelni



Źródło: Opracowanie własne na podstawie badań własnych

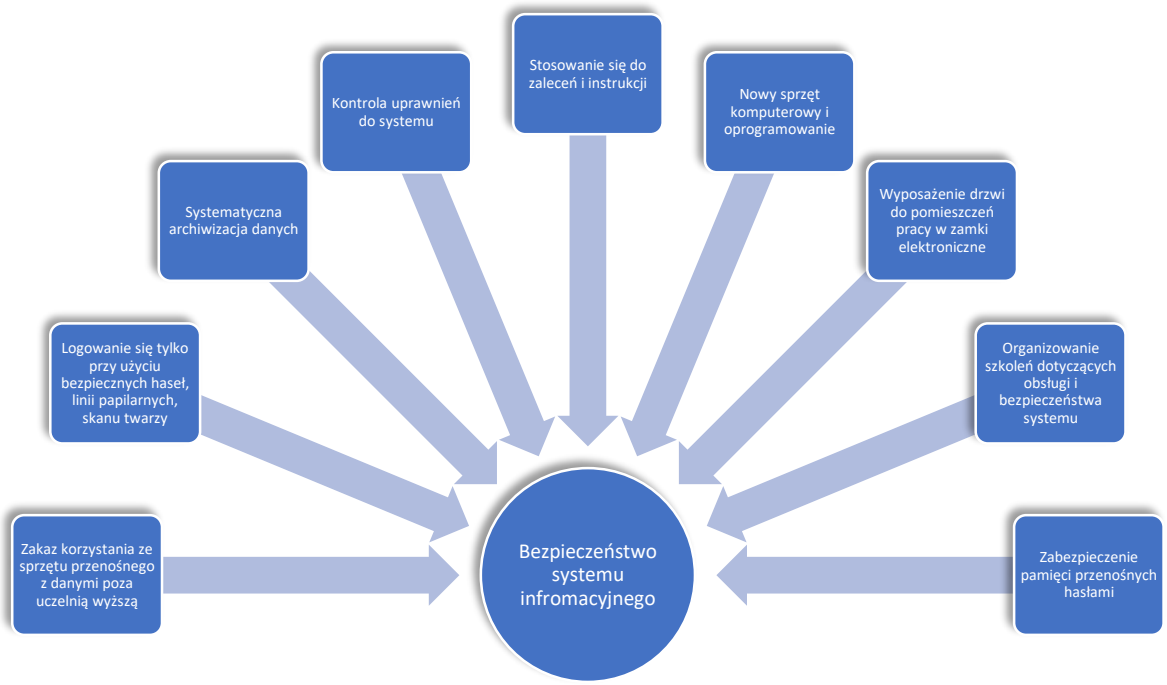
4.2. Zmiany w obszarze bezpieczeństwa systemu informacyjnego w uczelni wyższej

Koncepcja uwzględnia potrzebę eliminacji zagrożeń systemu informacyjnego w uczelni oraz ochronę, która byłaby systematyczna, wystarczająca i skuteczna. Należałoby wprowadzić wieloaspektowe rozwiązania obejmujące swoim zasięgiem wszystkich korzystających użytkowników systemu informacyjnego w uczelni wyższej.

Rysunek 4.4. przedstawia projekt elementów bezpieczeństwa systemu informacyjnego w uczelni wyższej. Proponowane do wdrożenia przez autorkę zmiany mają na celu wyeliminowanie obecnie występujących zagrożeń w bezpieczeństwie systemu informacyjnego w uczelni wyższej.

Proponowane zmiany swoim zakresem obejmują środowisko uczelniane, technologie informacyjne, procesy użytkowania informacji. W przeprowadzonych badaniach empirycznych ocenie została poddana opinia użytkowników i dotyczyła ona możliwości uzyskania większego poziomu bezpieczeństwa badanego systemu informacyjnego w uczelni wyższej.

Rysunek 4.4. Elementy bezpieczeństwa systemu informacyjnego w uczelni wyższej-projekt



Źródło: opracowanie własne

Za pomocą sondażu diagnostycznego w ramach oceny poziomu bezpieczeństwa informacji przez respondentów grupy nauczycieli akademickich, kadry administracyjnej, studentów (różnych roczników), ankietowani mieli możliwość wyboru jednej z dwóch zaproponowanych odpowiedzi „TAK" lub „NIE".

15. Czy Państwa zdaniem uzyskanie większego poziomu bezpieczeństwa systemu informacyjnego w uczelni wyższej jest możliwe poprzez:

- ograniczenie osobom nieupoważnionym dostępu do danych;
- zwiększenie świadomości wśród użytkowników o zagrożeniach jakie mogą wystąpić w konsekwencji niewłaściwego korzystania z systemu informacyjnego;
- zwiększenie kontroli użytkowników systemu informacyjnego;
- reagowanie na incydenty, związane z naruszeniem bezpieczeństwa systemu informacyjnego;
- zgłaszanie wszelkich zauważonych błędów i niedoskonałości systemowych;
- wykorzystanie nowoczesnego sprzętu komputerowego;
- stosowanie dobrze zabezpieczonych zewnętrznych nośników danych.

Tabela 4.28. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy kadra administracyjna na temat możliwości uzyskania większego poziomu bezpieczeństwa systemu informacyjnego w uczelni wyższej

ograniczenie osobom nieupoważnionym dostępu do danych						
Osoby poddane badaniu	**Respondenci nauczyciele akademiccy**		**Respondenci kadra administracyjna**		**OGÓŁEM**	
ODPOWIEDŹ	*liczba wskazań*	*udział procentowy*	*liczba wskazań*	*udział procentowy*	*liczba wskazań*	*udział procentowy*
TAK	500	100%	500	100%	1000	100%
NIE	0	0%	0	0%	0	0%
	500	100%	500	100%	1000	100%
zwiększenie świadomości wśród użytkowników o zagrożeniach jakie mogą wystąpić w konsekwencji niewłaściwego korzystania z systemu informacyjnego						
Osoby poddane badaniu	**Respondenci nauczyciele akademiccy**		**Respondenci kadra administracyjna**		**OGÓŁEM**	
ODPOWIEDŹ	*liczba wskazań*	*udział procentowy*	*liczba wskazań*	*udział procentowy*	*liczba wskazań*	*udział procentowy*
TAK	480	96%	500	100%	980	98%
NIE	10	2%	0	0%	10	1%
	500	100%	500	100%	1000	100%
zwiększenie kontroli użytkowników systemu informacyjnego						
Osoby poddane badaniu	**Respondenci nauczyciele akademiccy**		**Respondenci kadra administracyjna**		**OGÓŁEM**	
ODPOWIEDŹ	*liczba wskazań*	*udział procentowy*	*liczba wskazań*	*udział procentowy*	*liczba wskazań*	*udział procentowy*
TAK	478	95,6%	489	97,8%	967	96,7%
NIE	22	4,4%	11	2,2%	33	3,3%
	500	100%	500	100%	1000	100%
reagowanie na incydenty, związane z naruszeniem bezpieczeństwa systemu informacyjnego						
Osoby poddane badaniu	**Respondenci nauczyciele akademiccy**		**Respondenci kadra administracyjna**		**OGÓŁEM**	
ODPOWIEDŹ	*liczba wskazań*	*udział procentowy*	*liczba wskazań*	*udział procentowy*	*liczba wskazań*	*udział procentowy*
TAK	500	100%	500	100%	1000	100%
NIE	0	0%	0	0%	0	0%
	500	100%	500	100%	1000	100%
zgłaszanie wszelkich zauważonych błędów i niedoskonałości systemowych						
Osoby poddane badaniu	**Respondenci nauczyciele akademiccy**		**Respondenci kadra administracyjna**		**OGÓŁEM**	
ODPOWIEDŹ	*liczba wskazań*	*udział procentowy*	*liczba wskazań*	*udział procentowy*	*liczba wskazań*	*udział procentowy*
TAK	478	95,6%	500	100%	978	97,8%
NIE	22	4,4%	0	0	22	2,2%
	500	100%	500	100%	1000	100%
wykorzystanie nowoczesnego sprzętu komputerowego						
Osoby poddane badaniu	**Respondenci nauczyciele akademiccy**		**Respondenci kadra administracyjna**		**OGÓŁEM**	
ODPOWIEDŹ	*liczba wskazań*	*udział procentowy*	*liczba wskazań*	*udział procentowy*	*liczba wskazań*	*udział procentowy*
TAK	500	100%	500	100%	1000	100%
NIE	0	0%	0	0%	0	0

	500	100%	500	100%	1000	100%
stosowanie dobrze zabezpieczonych zewnętrznych nośników danych						
Osoby poddane badaniu	**Respondenci nauczyciele akademiccy**		**Respondenci kadra administracyjna**		**OGÓŁEM**	
ODPOWIEDŹ	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***
TAK	479	95,8%	496	99,2%	975	97,5%
NIE	21	4,2%	4	0,8%	25	2,5%
	500	100%	500	100%	100	100%

Źródło: opracowanie własne na podstawie badań własnych

Ogółem odpowiedzi udzieliło 100% respondentów z grupy nauczyciele akademiccy grupy kadra administracyjna. Z przeprowadzonej analizy wynika, że zarówno nauczyciele akademiccy jak i kadra administracyjna podzielają potrzebę zmian w celu zapewnienia bezpieczeństwa systemu informacyjnego w uczelni wyższej.

W ocenie ograniczenia osobom nieupoważnionym dostępu do danych opowiedziało się 100% respondentów z powyższej grupy badanej. Za zwiększeniem świadomości wśród użytkowników o zagrożeniach, jakie mogą wystąpić w konsekwencji niewłaściwego korzystania z systemu informacyjnego opowiedziało się 96% nauczycieli akademickich i 100% kadry administracyjnej, zaś 2% respondentów z grupy nauczycieli akademickich zaopiniowało negatywnie. Za zwiększeniem kontroli użytkowników systemu informacyjnego opowiedziało się 96,6% respondentów nauczycieli akademickich oraz 97,8% respondentów w grupie kadry administracyjnej. Były także osoby, które wyraziły się w sprzeczności, nauczyciele akademiccy 4,4% i kadra administracyjna 2,2%. Za reagowaniem na incydenty, związane z naruszeniem bezpieczeństwa systemu informacyjnego opowiedziało się 100% respondentów poddanych badaniom zarówno w grupie nauczycieli akademickich jak i w grupie kadry administracyjnej.

W opinii ankietowanych zgłaszanie wszelkich zauważonych błędów i niedoskonałości systemowych zostało pozytywnie zaopiniowane przez 95,6% respondentów w grupie nauczycieli akademickich i w 100% przez kadrę administracyjną, zaś 4,4% osób wyraziło niechęć, co do takich działań mających na celu wzmocnienie bezpieczeństwa systemu informacyjnego. Przy odpowiedzi na wykorzystanie nowoczesnego sprzętu komputerowego, pozytywnie w 100% wypowiedziała się zarówno grupa nauczycieli akademickich i grupy kadry administracyjnej. Respondenci grupy nauczycieli akademickich w 95,8% optowali za stosowaniem dobrze zabezpieczonych zewnętrznych nośników danych a w grupie kadry administracyjnej było to 99,2%. Negatywnie wypowiedziało się łącznie tylko 25 osób, co daje w przeliczeniu procentowym 2,5%.

Ranga 1:

- ograniczenie osobom nieupoważnionym dostępu do danych;
- reagowanie na incydenty, związane z naruszeniem bezpieczeństwa systemu informacyjnego;
- wykorzystanie nowoczesnego sprzętu komputerowego;

Ranga 2:

- zwiększenie świadomości wśród użytkowników o zagrożeniach jakie mogą wystąpić w konsekwencji niewłaściwego korzystania z systemu informacyjnego;

Ranga 3:

- zgłaszanie wszelkich zauważonych błędów i niedoskonałości systemowych;

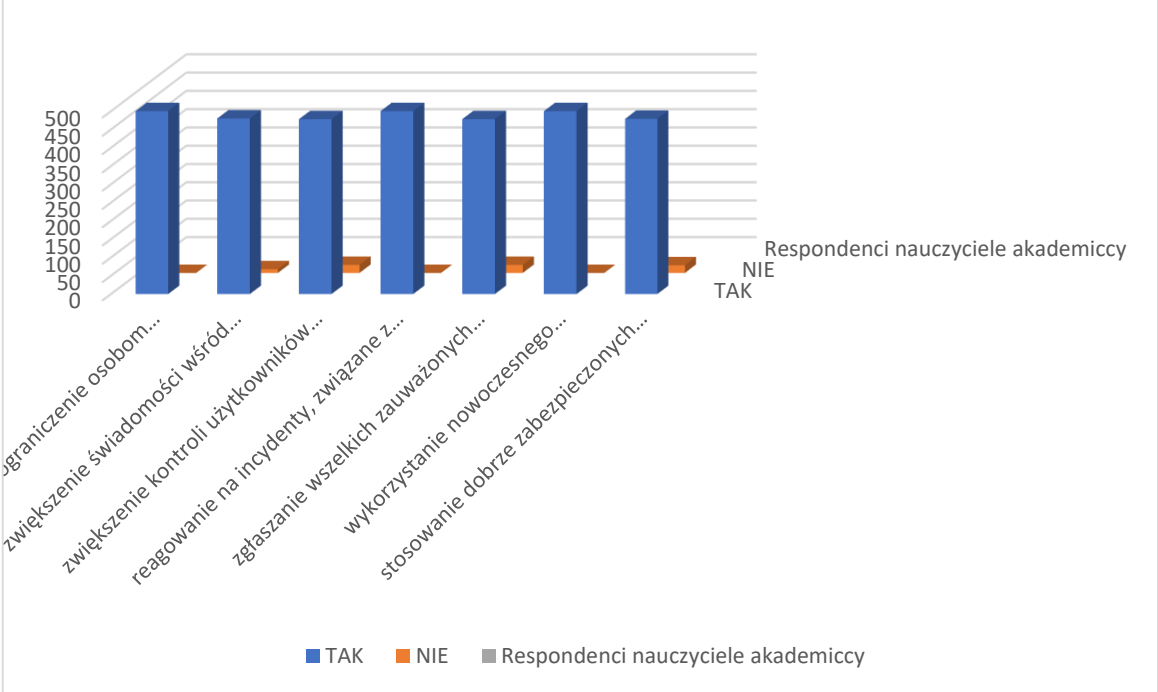
Ranga 4:

- stosowanie dobrze zabezpieczonych zewnętrznych nośników danych

Ranga 5:

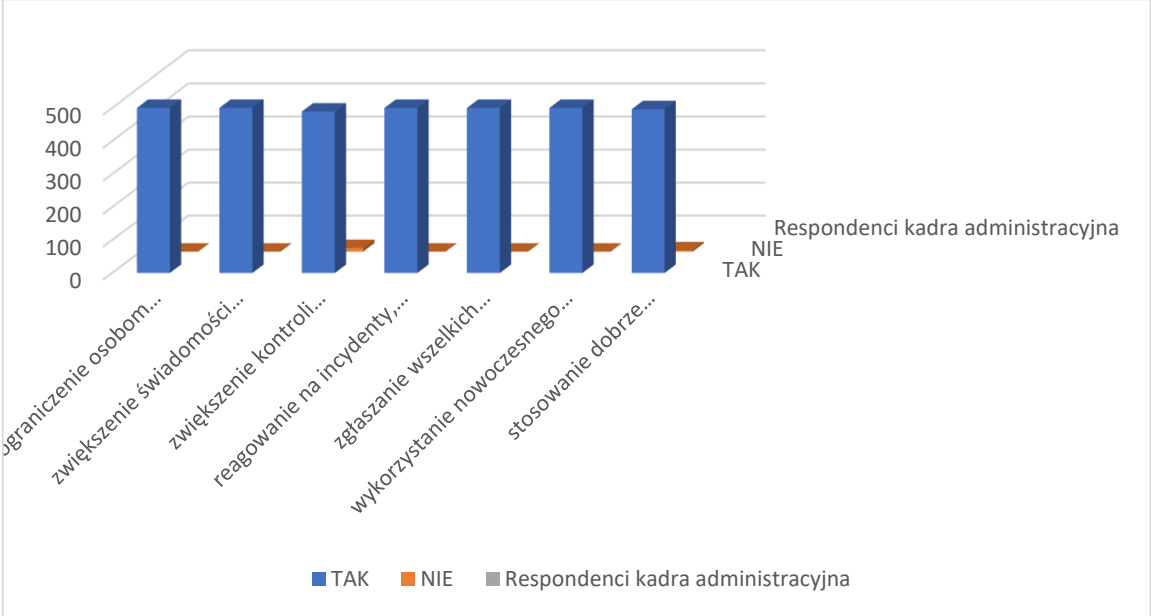
- zwiększenie kontroli użytkowników systemu informacyjnego.

Wykres 4.55. Odpowiedzi respondentów grupy nauczyciele akademiccy na temat możliwości uzyskania większego poziomu bezpieczeństwa systemu informacyjnego w uczelni wyższej



Źródło: opracowanie własne na podstawie badań własnych

Wykres 4.56. Odpowiedzi respondentów grupy kadra administracyjna na temat możliwości uzyskania większego poziomu bezpieczeństwa systemu informacyjnego w uczelni wyższej



Źródło: opracowanie własne na podstawie badań własnych

Tabela 4.29. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy studenci (różne kierunki) na temat możliwości uzyskania większego poziomu bezpieczeństwa systemu informacyjnego w uczelni wyższej

ograniczenie osobom nieupoważnionym dostępu do danych						
Osoby poddane badaniu	**Respondenci nauczyciele akademiccy**		**Respondenci studenci (różne kierunki)**		**OGÓŁEM**	
ODPOWIEDŹ	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***
TAK	500	100%	328	65,6%	828	82,8%
NIE	0	0%	172	34,4%	172	17,2%
	500	100%	500	100%	1000	100%
zwiększenie świadomości wśród użytkowników o zagrożeniach jakie mogą wystąpić w konsekwencji niewłaściwego korzystania z systemu informacyjnego						
Osoby poddane badaniu	**Respondenci nauczyciele akademiccy**		**Respondenci studenci (różne kierunki)**		**OGÓŁEM**	
ODPOWIEDŹ	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***
TAK	480	96%	285	57%	765	76,5%
NIE	10	2%	215	43%	225	22,5%
	500	100%	500	100%	1000	100%
zwiększenie kontroli użytkowników systemu informacyjnego						
Osoby poddane badaniu	**Respondenci nauczyciele akademiccy**		**Respondenci studenci (różne kierunki)**		**OGÓŁEM**	
ODPOWIEDŹ	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***
TAK	478	95,6%	279	55,8%	757	75,7%
NIE	22	4,4%	221	44,2%	243	24,3%
	500	100%	500	100%	1000	100%
reagowanie na incydenty, związane z naruszeniem bezpieczeństwa systemu informacyjnego						

Osoby poddane badaniu	Respondenci nauczyciele akademiccy		Respondenci studenci (różne kierunków)		OGÓŁEM	
ODPOWIEDŹ	*liczba wskazań*	*udział procentowy*	*liczba wskazań*	*udział procentowy*	*liczba wskazań*	*udział procentowy*
TAK	500	100%	381	76,2%	881	88,1%
NIE	0	0%	119	23,8%	119	11,9%
	500	100%	500	100%	1000	100%
zgłaszanie wszelkich zauważonych błędów i niedoskonałości systemowych						
Osoby poddane badaniu	**Respondenci nauczyciele akademiccy**		**Respondenci studenci (różne kierunki)**		**OGÓŁEM**	
ODPOWIEDŹ	*liczba wskazań*	*udział procentowy*	*liczba wskazań*	*udział procentowy*	*liczba wskazań*	*udział procentowy*
TAK	478	95,6%	392	78,4%	870	87%
NIE	22	4,4%	108	21,6%	130	13%
	500	100%	500	100%	1000	100%
wykorzystanie nowoczesnego sprzętu komputerowego						
Osoby poddane badaniu	**Respondenci nauczyciele akademiccy**		**Respondenci studenci (różne kierunki)**		**OGÓŁEM**	
ODPOWIEDŹ	*liczba wskazań*	*udział procentowy*	*liczba wskazań*	*udział procentowy*	*liczba wskazań*	*udział procentowy*
TAK	500	100%	426	85,2%	926	92,6%
NIE	0	0%	74	14,8%	74	7,4
	500	100%	500	100%	1000	100%
stosowanie dobrze zabezpieczonych zewnętrznych nośników danych						
Osoby poddane badaniu	**Respondenci nauczyciele akademiccy**		**Respondenci studenci (różne kierunki)**		**OGÓŁEM**	
ODPOWIEDŹ	*liczba wskazań*	*udział procentowy*	*liczba wskazań*	*udział procentowy*	*liczba wskazań*	*udział procentowy*
TAK	479	95,8%	356	71,2%	835	83,5%
NIE	21	4,2%	144	28,8%	165	16,5%
	500	100%	500	100%	100	100%

Źródło: opracowanie własne na podstawie badań własnych

W badaniu wzięło udział 100 % respondentów w grupie studentów (różnych kierunków). W opinii studentów za ograniczeniem osobom nieupoważnionym dostępu do danych opowiedziało się 65,6% respondentów a przeciw było 34,4%. Zwiększenie świadomości wśród użytkowników o zagrożeniach, jakie mogą wystąpić w konsekwencji niewłaściwego korzystania z systemu informacyjnego, pozytywnie wypowiedziało się 57% osób a przeciw było 43%. Za zwiększeniem kontroli użytkowników systemu informacyjnego w opinii respondentów w grupie studentów wypowiedziało się pozytywnie 55,8% a negatywnie w tym temacie zaopiniowało 44,2% studentów.

Na temat reagowania na incydenty, związane z naruszeniem bezpieczeństwa systemu informacyjnego opowiedziało się pozytywnie 76,2% respondentów z grupy badanych studentów, zaś odmiennego zdania miało 23,8%. Duża ilość studentów pozytywnie

zapatruje się na zgłaszanie wszelkich zauważonych błędów i niedoskonałości systemowych i tu, za tą odpowiedzią było 78,4% ankietowanych a przeciw 21,6%. Ważnym działaniem także w kształceniu studentów jest wykorzystanie nowoczesnego sprzętu komputerowego i tu w opinii respondentów tej grupy 85,2% osób było za a 14,8% przeciw 71,2% studentów chciałoby stosowania dobrze zabezpieczonych zewnętrznych nośników danych, ale było także 28,8% osób, które uważały, że nie jest to konieczne.

Ranga 1:

- wykorzystanie nowoczesnego sprzętu komputerowego;

Ranga 2:

- reagowanie na incydenty, związane z naruszeniem bezpieczeństwa systemu informacyjnego;

Ranga 3:

- zgłaszanie wszelkich zauważonych błędów i niedoskonałości systemowych;

Ranga 4:

- stosowanie dobrze zabezpieczonych zewnętrznych nośników danych

Ranga 5:

- ograniczenie osobom nieupoważnionym dostępu do danych;

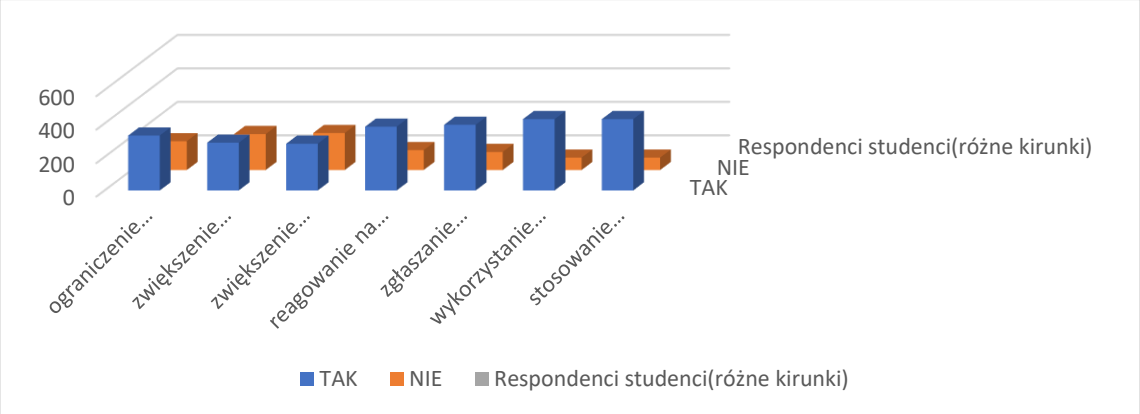
Ranga 6:

- zwiększenie świadomości wśród użytkowników o zagrożeniach, jakie mogą wystąpić w konsekwencji niewłaściwego korzystania z systemu informacyjnego;

Ranga 7:

- zwiększenie kontroli użytkowników systemu informacyjnego.

Wykres 4.57. Odpowiedzi respondentów grupy studenci (różne kierunki) na temat możliwości uzyskania większego poziomu bezpieczeństwa systemu informacyjnego w uczelni wyższej



Źródło: opracowanie własne na podstawie badań własnych

Tabela 4.30. Odpowiedzi respondentów grupy kadra administracyjna i grupy studenci (różne kierunki) na temat możliwości uzyskania większego poziomu bezpieczeństwa systemu informacyjnego w uczelni wyższej

ograniczenie osobom nieupoważnionym dostępu do danych						
Osoby poddane badaniu	**Respondenci kadra administracyjna**		**Respondenci studenci (różne kierunki)**		**OGÓŁEM**	
ODPOWIEDŹ	*liczba wskazań*	*udział procentowy*	*liczba wskazań*	*udział procentowy*	*liczba wskazań*	*udział procentowy*
TAK	500	100%	328	65,6%	828	82,8%
NIE	0	0%	172	34,4%	172	17,2%
	500	100%	500	100%	1000	100%
zwiększenie świadomości wśród użytkowników o zagrożeniach, jakie mogą wystąpić w konsekwencji niewłaściwego korzystania z systemu informacyjnego						
Osoby poddane badaniu	**Respondenci kadra administracyjna**		**Respondenci studenci (różne kierunki)**		**OGÓŁEM**	
ODPOWIEDŹ	*liczba wskazań*	*udział procentowy*	*liczba wskazań*	*udział procentowy*	*liczba wskazań*	*udział procentowy*
TAK	500	100%	285	57%	785	78,5%
NIE	0	0%	215	43%	215	21,5%
	500	100%	500	100%	1000	100%
zwiększenie kontroli użytkowników systemu informacyjnego						
Osoby poddane badaniu	**Respondenci kadra administracyjna**		**Respondenci studenci (różne kierunki)**		**OGÓŁEM**	
ODPOWIEDŹ	*liczba wskazań*	*udział procentowy*	*liczba wskazań*	*udział procentowy*	*liczba wskazań*	*udział procentowy*
TAK	489	97,8%	279	55,8%	768	76,8%
NIE	11	2,2%	221	44,2%	232	23,2%
	500	100%	500	100%	1000	100%
reagowanie na incydenty, związane z naruszeniem bezpieczeństwa systemu informacyjnego						
Osoby poddane badaniu	**Respondenci kadra administracyjna**		**Respondenci studenci (różne kierunków)**		**OGÓŁEM**	
ODPOWIEDŹ	*liczba wskazań*	*udział procentowy*	*liczba wskazań*	*udział procentowy*	*liczba wskazań*	*udział procentowy*
TAK	500	100%	381	76,2%	881	88,1%
NIE	0	0%	119	23,8%	119	11,9%
	500	100%	500	100%	1000	100%
zgłaszanie wszelkich zauważonych błędów i niedoskonałości systemowych						
Osoby poddane badaniu	**Respondenci kadra administracyjna**		**Respondenci studenci (różne kierunki)**		**OGÓŁEM**	

ODPOWIEDŹ	*liczba wskazań*	*udział procentowy*	*liczba wskazań*	*udział procentowy*	*liczba wskazań*	*udział procentowy*
TAK	500	100%	392	78,4%	892	89,2%
NIE	0	0%	108	21,6%	108	10,8%
	500	100%	500	100%	1000	100%
wykorzystanie nowoczesnego sprzętu komputerowego						
Osoby poddane badaniu	**Respondenci kadra administracyjna**		**Respondenci studenci (różne kierunki)**		**OGÓŁEM**	
ODPOWIEDŹ	*liczba wskazań*	*udział procentowy*	*liczba wskazań*	*udział procentowy*	*liczba wskazań*	*udział procentowy*
TAK	500	100%	426	85,2%	926	92,6%
NIE	0	0%	74	14,8%	74	7,4
	500	100%	500	100%	1000	100%
stosowanie dobrze zabezpieczonych zewnętrznych nośników danych						
Osoby poddane badaniu	**Respondenci kadra administracyjna**		**Respondenci studenci (różne kierunki)**		**OGÓŁEM**	
ODPOWIEDŹ	*liczba wskazań*	*udział procentowy*	*liczba wskazań*	*udział procentowy*	*liczba wskazań*	*udział procentowy*
TAK	496	99,2%	356	71,2%	852	85,2%
NIE	4	0,8%	144	28,8%	148	14,8%
	500	100%	500	100%	100	100%

Źródło: opracowanie własne na podstawie badań własnych

Ranga 1:

- wykorzystanie nowoczesnego sprzętu komputerowego;

Ranga 2:

- zgłaszanie wszelkich zauważonych błędów i niedoskonałości systemowych;

Ranga 3:

- reagowanie na incydenty, związane z naruszeniem bezpieczeństwa systemu informacyjnego;

Ranga 4:

- stosowanie dobrze zabezpieczonych zewnętrznych nośników danych;

Ranga 5:

- ograniczenie osobom nieupoważnionym dostępu do danych;

Ranga 6:

- zwiększenie świadomości wśród użytkowników o zagrożeniach, jakie mogą wystąpić w konsekwencji niewłaściwego korzystania z systemu informacyjnego;

Ranga 7:

- zwiększenie kontroli użytkowników systemu informacyjnego.

Podsumowując, w przeważającej większości użytkownicy systemu informacyjnego uczelni wyższej dostrzegają niedoskonałości w bezpieczeństwie systemu informacyjnego.

W sposób jednomyślny 3 grupy nauczyciele akademiccy, kadra administracyjna, studenci różne kierunki wskazały na potrzebę wykorzystania nowoczesnego sprzętu komputerowego.

W każdej sferze niska świadomość zagrożeń może powodować bardzo duże konsekwencje. W odpowiedziach respondentów zasygnalizowany jest fakt zwiększenia świadomości wśród użytkowników o zagrożeniach, jakie mogą wystąpić w konsekwencji niewłaściwego korzystania z systemu informacyjnego. Brakuje także sprawczości reagowania na incydenty, związane z naruszeniem bezpieczeństwa systemu informacyjnego.

Często dochodzi do sytuacji, w której bagatelizowane są zgłoszenia odnośnie naruszeń, a to powoduje, że użytkownicy wychodzą z założenia o bezcelowości zgłaszania takich zdarzeń. Dlatego też w koncepcji reagowania na powstałe incydenty związane z naruszeniami bezpieczeństwa systemu informacyjnego w uczelni wyższej powinno być standardem. Podobny rozdźwięk w teorii i praktyce pojawia się przy ograniczeniu osobom nieupoważnionym dostępu do danych. Jak dowiodły badania, istnieje potrzeba zapewnienia bezpieczeństwa w uczelni wyższej.

Badania wykazały, że w końcowych rangach znalazła się odpowiedź dotycząca zwiększenia kontroli użytkowników systemu informacyjnego. Wszystkie wspomniane aspekty wydają się oczywiste i zrozumiałe, jednak właśnie ta oczywistość zmyliła władze uczelni wyższej. Wśród tak zróżnicowanych grup użytkowników o różnych m.in. poziomach wiedzy, kompetencji, wieku nie można uznawać, że jeżeli coś zostało spisane w formie instrukcji czy procedur to będzie to w prawidłowy sposób funkcjonować.

W badaniach empirycznych ocenie został poddany pogląd użytkowników na temat bezpieczeństwa systemu informacyjnego w uczelni wyższej. Za pomocą sondażu diagnostycznego w ramach oceny poglądu na temat stopnia bezpieczeństwa systemu informacyjnego przez respondentów grupy nauczyciele akademiccy, kadra administracyjna, studenci (różne kierunki) ankietowani mieli możliwość udzielenia jednej z pięciu zaproponowanych odpowiedzi:

17. Jaka jest Państwa ogólna ocena bezpieczeństwa systemu informacyjnego w uczelni wyższej? Tabela 4.31. przedstawia rozkład odpowiedzi respondentów grupy nauczyciele akademiccy i grupy kadra administracyjna.

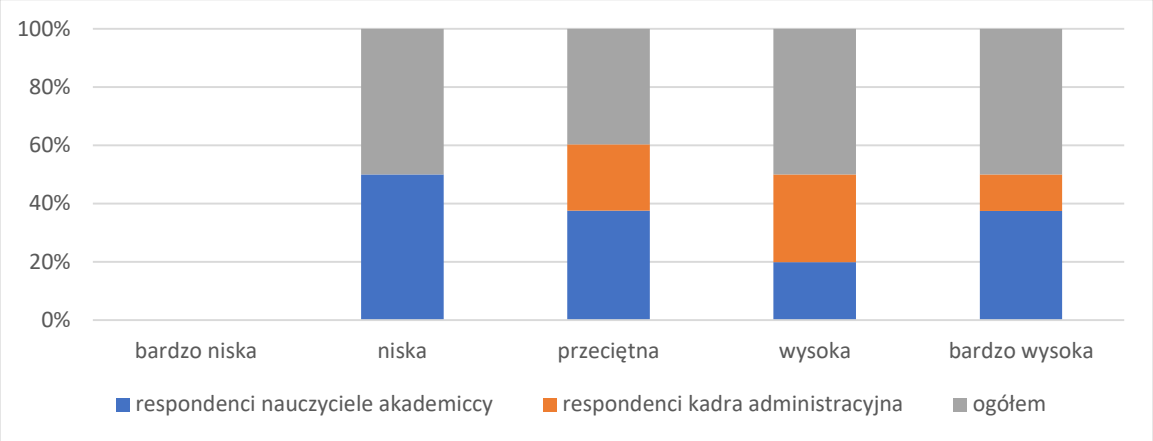
Tabela 4.31. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy kadra administracyjna na temat stopnia bezpieczeństwa systemu informacyjnego w uczelni wyższej

Odpowiedzi badanych osób *stopień bezpieczeństwa systemu informacyjnego w uczelni wyższej*						
Osoby poddane badaniu	**Respondenci nauczyciele akademiccy**		**Respondenci kadra administracyjna**		**OGÓŁEM**	
Odpowiedź	*liczba wskazań*	*udział procentowy*	*liczba wskazań*	*udział procentowy*	*liczba wskazań*	*udział procentowy*
bardzo niska	0	0%	0	0%	0	0%
niska	6	1,2%	0	0%	6	0,6%
przeciętna	214	42,8%	129	25,8%	226	22,6%
wysoka	235	47%	356	71,2%	591	59,1%
bardzo wysoka	45	9%	15	3%	60	6%
	500	**100%**	**500**	**100%**	**1000**	**100%**

Źródło: opracowanie własne na podstawie badań własnych

Na pytanie 17 kwestionariusza ankiety wypowiedziało się 100% respondentów badanej zbiorowości. W grupie nauczycieli akademickich najwyższą zadeklarowaną odpowiedzią na pytanie o stopień bezpieczeństwa systemu informacyjnego w uczelni wyższej była odpowiedź „wysoka" i na tą odpowiedź zdecydowało się 47% osób, za odpowiedzią „bardzo niska" w tej grupie respondentów nikt się nie opowiedział. Kadra administracyjna tak samo jak nauczyciele akademiccy określiła stopień bezpieczeństwa systemu informacyjnego, jako wysoki i było to 71,2% respondentów. Nikt z grupy kadry administracyjnej nie wskazał odpowiedzi „bardzo niska".

Wykres 4.58. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy kadra administracyjna na temat stopnia bezpieczeństwa systemu informacyjnego w uczelni wyższej



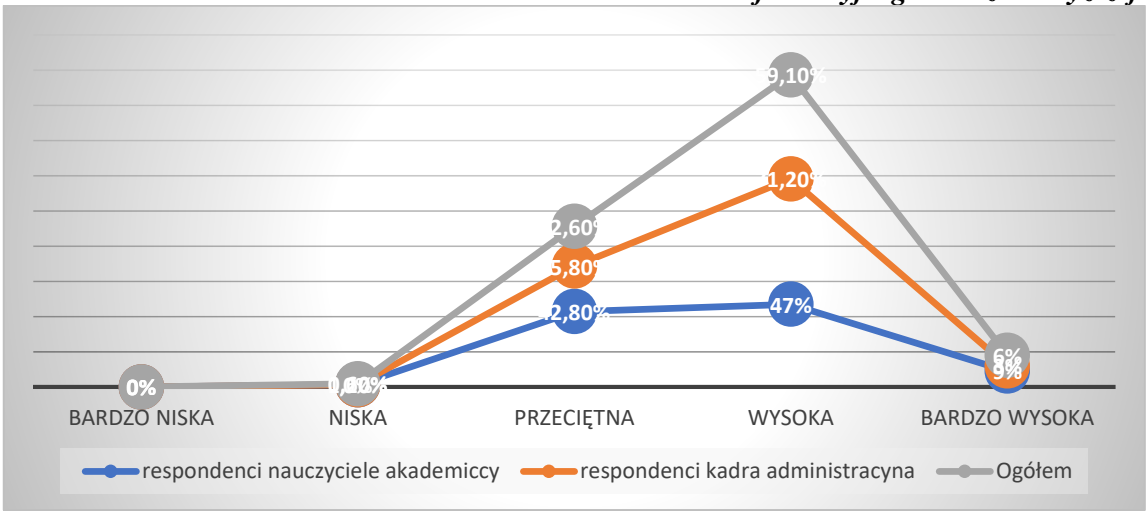
Źródło: opracowanie własne na podstawie badań własnych

O stopniu zależności decyduje współczynnik korelacji liniowej Pearsona na poziomie 0,88 i współczynnik determinacji liniowej, który wskazuje procent wyjaśnionej liniowo zmienności równy 77,44%.

$$r_{xy} = \frac{\frac{1}{n}\sum_{i=1}^{n}(x_i-\bar{x})(y_i-\bar{y})}{S_x S_y}=0{,}88$$

$$\text{WD}=r_{xy}^{2} * 100\% = 77{,}44\%$$

Wykres 4.59. Zależność między respondentami grupy nauczyciele akademiccy i grupy kadra administracyjna pod względem stopnia bezpieczeństwa systemu informacyjnego w uczelni wyższej



Źródło: opracowanie własne na podstawie badań własnych

W tym przypadku należy stwierdzić, że występująca korelacja pomiędzy zmiennymi jest silna. W opinii grupy nauczycieli akademickich i grupy kadry administracyjnej

potwierdza się wystąpienie bezpieczeństwa systemu informacyjnego w uczelni wyższej. W tabeli 4.32. został zaprezentowany rozkład odpowiedzi dotyczący oceny przez użytkowników, stopnia bezpieczeństwa systemu informacyjnego w uczelni wyższej. W ocenie wzięły udział dwie grupy respondentów, nauczyciele akademiccy i studenci (różne kierunki).

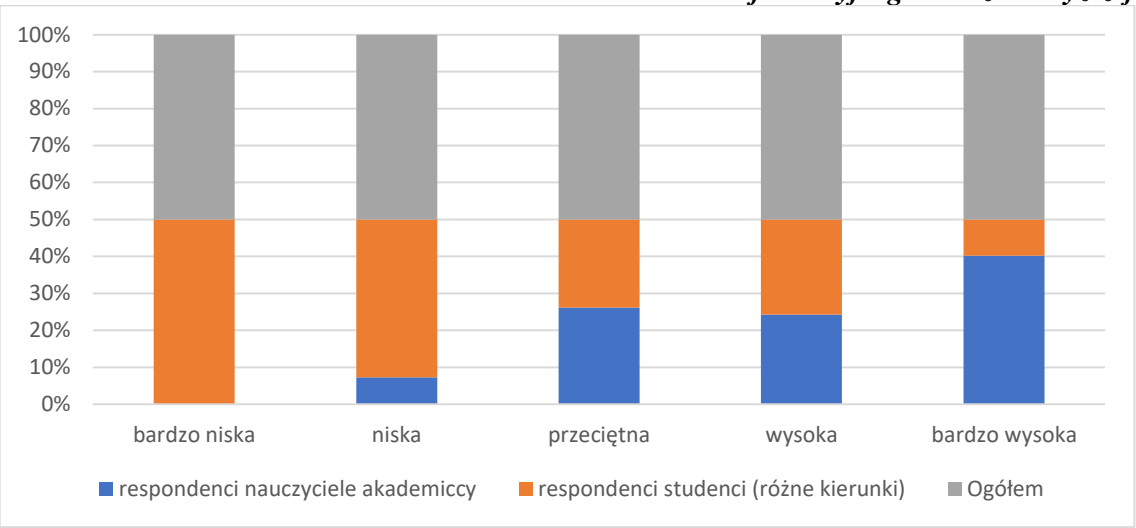
Tabela 4.32. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy studenci (różne kierunki) na temat stopnia bezpieczeństwa systemu informacyjnego w uczelni wyższej

Odpowiedzi badanych osób *stopień bezpieczeństwa systemu informacyjnego w uczelni wyższej*						
Osoby poddane badaniu	**Respondenci nauczyciele akademiccy**		**Respondenci studenci (różne kierunki)**		**OGÓŁEM**	
Odpowiedź	*liczba wskazań*	*udział procentowy*	*liczba wskazań*	*udział procentowy*	*liczba wskazań*	*udział procentowy*
bardzo niska	0	0%	9	1,8%	9	0,9%
niska	6	1,2%	35	7%	41	4,1%
przeciętna	214	42,8%	195	39%	409	40,9%
wysoka	235	47%	250	50%	485	48,5%
bardzo wysoka	45	9%	11	2,2%	56	5,6%
	500	**100%**	**500**	**100%**	**1000**	**100%**

Źródło: Opracowanie własne na podstawie badań własnych

Z danych empirycznych wynika, że 47% nauczycieli akademickich i 50% studentów oceniło bezpieczeństwo systemu informacyjnego na poziomie wysokim. Zdaniem 6% nauczycieli akademickich powyższy system został oceniony na bardzo niskim poziomie. W populacji studentów 1,8% respondentów poddanych ocenie, system oceniło na bardzo niski poziomie a 7% uważa, że ten stopień bezpieczeństwa sytemu informacyjnego w uczelni wyższej jest niski.

Wykres 4.60. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy studenci (różne kierunki) na temat stopnia bezpieczeństwa systemu informacyjnego w uczelni wyższej



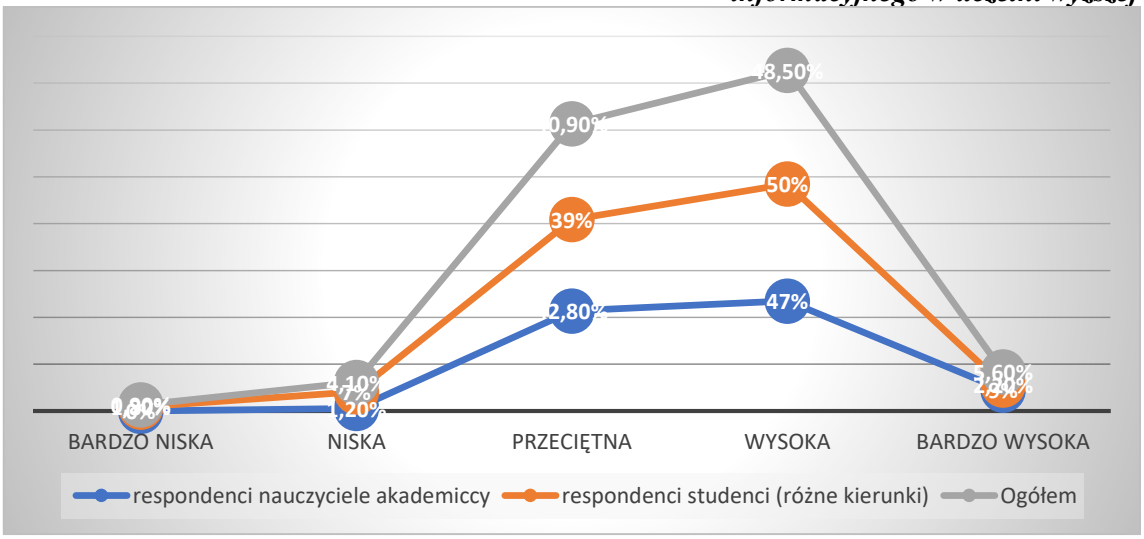
Źródło: opracowanie własne na podstawie badań własnych

Na zależność korelacji wskazuje współczynnik korelacji liniowej Pearsona na poziomie 0,97 i współczynnik determinacji liniowej, który przedstawia procent wyjaśnionej liniowo zmienności i jest równy 94,09.

$$r_{xy} = \frac{\frac{1}{n}\sum_{i=1}^{n}(x_i-\bar{x})(y_i-\bar{y})}{S_x S_y}=0{,}97$$

$$\mathrm{WD}=r_{xy}^{2} * 100\% = 94{,}09\%$$

Wykres 4.61. Zależność między respondentami grupy nauczyciele akademiccy i grupy studenci (różne kierunki) pod względem stopnia bezpieczeństwa systemu informacyjnego w uczelni wyższej



Źródło: opracowanie własne na podstawie badań własnych

Wykres ten pokazuje silną korelację dodatnią wśród grupy nauczycieli akademickich i grupy studentów. Oznacza to, że w opinii tych badanych grup respondentów występuje bezpieczeństwo informacyjne w uczelni wyższej. Rozkład odpowiedzi na temat oceny stopnia bezpieczeństwa systemu informacyjnego w uczelni wyższej w opinii grupy kadra administracyjna i grupy studentów (różnych kierunków) została przedstawiona w tabeli 4.33.

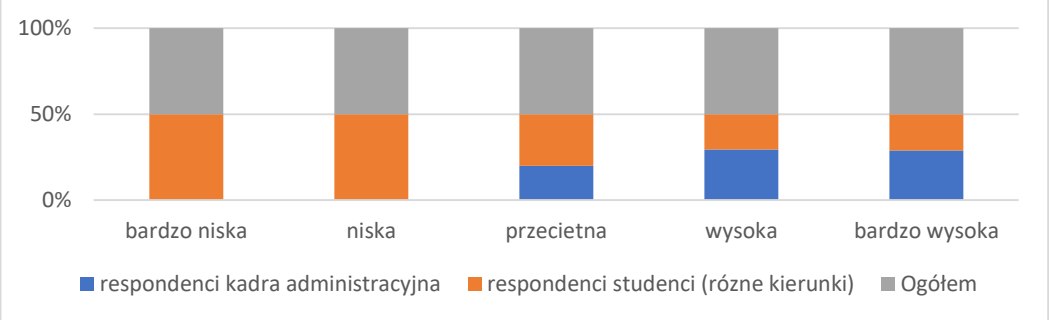
Tabela 4.33. Odpowiedzi respondentów grupy kadra administracyjna i grupy studenci (różne kierunki) na temat stopnia bezpieczeństwa systemu informacyjnego w uczelni wyższej

Odpowiedzi badanych osób *stopień bezpieczeństwa systemu informacyjnego w uczelni wyższej*						
Osoby poddane badaniu	**Respondenci kadra administracyjna**		**Respondenci studenci (różne kierunki)**		**OGÓŁEM**	
Odpowiedź	*liczba wskazań*	*udział procentowy*	*liczba wskazań*	*udział procentowy*	*liczba wskazań*	*udział procentowy*
bardzo niska	0	0%	9	1,8%	9	0,9%
niska	0	0%	35	7%	35	3,5%
przeciętna	129	25,8%	195	39%	324	32,4%
wysoka	356	71,2%	250	50%	606	60,6%
bardzo wysoka	15	3%	11	2,2%	26	2,6%
	500	**100%**	**500**	**100%**	**1000**	**100%**

Źródło: opracowanie własne na podstawie badań własnych

Z wyników badań wynika, że kadra administracyjna tak jak i studenci uważa, że stopień bezpieczeństwa systemu informacyjnego w uczelni wyższej jest na wysokim poziomie. 15% respondentów w grupie kadry administracyjnej określiło ten stopień bezpieczeństwa, jako bardzo wysoki i 11% respondentów w grupie studentów.

Wykres 4. 62. Odpowiedzi respondentów grupy kadra administracyjna i grupy studenci (różne kierunki) na temat stopnia bezpieczeństwa systemu informacyjnego w uczelni wyższej



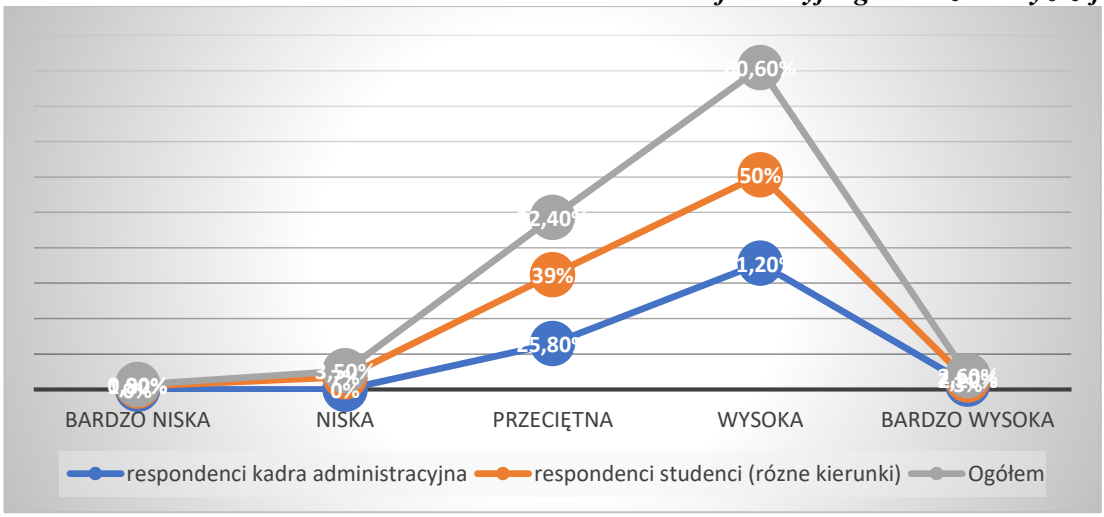
Źródło: opracowanie własne na podstawie badań własnych

Istnieje zależność pomiędzy badanymi grupami a decyduje o niej współczynnik korelacji liniowej Pearsona na poziomie 0,92 i współczynnik determinacji liniowej, wskazujący procent wyjaśnionej liniowo zmienności równy 84,64%.

$$r_{xy} = \frac{\frac{1}{n}\sum_{i=1}^{n}(x_i-\bar{x})(y_i-\bar{y})}{s_x s_y}=0{,}92$$

$$\mathrm{WD}=r_{xy}^{2} * 100\% = 84{,}64\%$$

Wykres 4.63. Zależność między respondentami grupy kadra administracyjna i grupy studenci (różne kierunki) pod względem stopnia bezpieczeństwa systemu informacyjnego w uczelni wyższej



Źródło: opracowanie własne na podstawie badań własnych

Dokonując analizy zależności widać, że korelacja pomiędzy obiema grupami, kadrą administracyjną i studentami różnych kierunków jest bardzo silna. W opinii kadry administracyjnej i studentów jest zachowany stopień bezpieczeństwa informacyjnego w uczelni wyższej.

Podsumowując, studenci bardziej obiektywnie ocenili bezpieczeństwo systemu informacyjnego w uczelni wyższej niż pozostałe dwie grupy. Wynikać to może z podporządkowania obowiązującym normom, regułom i standardom panującym w uczelni wyższej. Natomiast kadra administracyjna nie była w pełni obiektywna w swojej wysokiej ocenie, gdyż ta grupa respondentów nie chciała uzewnętrznić problemu z nie w pełni wykształconym poziomem bezpieczeństwa systemu informacyjnego w uczelni wyższej. Podobna reakcja na powyższy temat była taka sama wśród grupy nauczycieli akademickich.

ZAKOŃCZENIE

Przeprowadzone działania pozwoliły na rozwiązanie problemu badawczego odpowiadającego na pytanie:, Jakie ***uwarunkowania wpływają na bezpieczeństwo systemu informacyjnego w uczelni wyższej?*** i weryfikację przyjętej w pracy hipotezy, mającej w założeniu, iż ***obecny system informacyjny w organizacji publicznej na przykładzie uczelni wyższej nie w pełni chroni informację***. Oczywistym jest fakt, że to właśnie władze uczelni i kierownicy jednostek organizacyjnych powinni zwiększyć kontrolę nad działaniami wykonywanymi w systemie informacyjnym, szkoleniami pracowników, aby zapewnić pełne bezpieczeństwo użytkowników systemu informacyjnego. Uczelnia, jako organizacja kształcąca studentów i zatrudniająca pracowników powinna wprowadzić takie zabezpieczenia systemowe, które powodowałyby blokowanie logowań do kont (e-mailowych) prywatnych. Wiadomości powinny być przesyłane z kont pracowników mających domenę uczelnianą. Studenci kształcący się w uczelni wyższej tak jak i pracownicy powinni być poinstruowani o konieczności korzystania ze swoich e-maili studenckich.

Powyższa procedura ma na celu szybką weryfikację czy dana osoba jest powiązana bezpośrednio z uczelnią. W innym przypadku nie ma możliwości zweryfikowania takiej osoby a co za tym idzie udzielanie odpowiedzi za pośrednictwem innych adresów e-mailowych może stać się zagrożeniem zwłaszcza w sytuacji przesyłania ważnych materiałów, skanów dokumentacji, o którą poprosiła inna osoba. Potrzebnym a nawet wymaganym działaniem powinien być zakaz wynoszenia na zewnątrz laptopów zawierających dane osobowe, których utrata mogłaby działać na niekorzyść pracownika a co za tym idzie jednostki czy w szerszym pojęciu całej organizacji.

Uprawnienia do systemów powinni otrzymywać pracownicy, którzy danym zakresem działań będą się zajmować, na co dzień i posiadają to w zaktualizowanym zakresie swoich obowiązków. Pod uwagę brane są dane wrażliwe, których utrata może powodować zagrożenie. Dyski oraz urządzenia powinny posiadać hasła w przypadku zagubienia nie ma do nich łatwego dostępu. Ważnym aspektem jest ciągłe wdrażanie procedur i zabezpieczeń informacji.

Droga elektroniczna w szczególności e-maile pracownicze powinny być szczególnie zabezpieczone, aby nie dochodziło do przepuszczania tzw. spamu z różnego rodzaju reklamami, linkami mogącymi zawierać wirusy. W celu zwiększenia bezpieczeństwa systemu informacyjnego należy zakupić specjalne oprogramowania, zakupić nowy sprzęt a zamortyzować ten, który jest już leciwy. Taki sprzęt szybko ulega wszelkim awariom a dane na nim zapisane mogą ulec utraceniu. Przestaje on też spełniać swoje funkcje poprzez „zawodność", co może zdezorganizować pracę.

Współczesne trendy w wyszukiwaniu innowacyjnych rozwiązań teleinformatycznych obligują do utrzymania wysokich standardów bezpieczeństwa systemu informacyjnego na etapie wynalazczości. Jest to czas związany z administrowaniem sieci, systemów komputerowych jak i ustawicznego szkolenia wszystkich użytkowników tego systemu. Utrzymanie bezpieczeństwa w przypadku systemu informacyjnego wymaga ciągłego i niezmiennego dostosowywania się do najnowszych wynalazków cyfryzacji. Rozwój społeczeństwa informacyjnego jest bardzo intensywny i szybki, co ma pozytywne przełożenie na zwiększoną potrzebę wdrażania systemów informacyjnych dla ułatwienia funkcjonowania człowieka w ówczesnym społeczeństwie. Nakłady finansowe na zakup nowocześniejszych komputerów, urządzeń, oprogramowań oraz Internet i rozbudowane systemy informacyjne, informatyczne, uważane są za właściwy kierunek rozwoju całego społeczeństwa jak i w tym przypadku organizacji, jaką jest publiczna uczelnia wyższa. Jednakże użytkowanie tych dóbr staje się coraz częściej obiektem zainteresowań środowisk przestępczych i zachowań nie zgodnych z obowiązującym prawem.

Powyższe przemyślenia skłoniły autorkę do podjęcia próby zbadania bezpieczeństwa systemu informacyjnego w organizacji publicznej, jaką jest uczelnia wyższa. Podstawowe założenie dysertacji to opracowanie koncepcji bezpieczeństwa systemu informacyjnego w uczelni wyższej, w celu zwiększenia efektywności i skuteczności zabezpieczeń informacji. Rozwiązanie problemów szczegółowych i pozytywne zweryfikowanie hipotez szczegółowych umożliwiło rozwiązanie głównego problemu badawczego zawartego w pytaniu:, Jakie ***zmiany należy wprowadzić w bezpieczeństwie systemu informacyjnego w uczelni wyższej, aby poprawić skuteczność ochrony informacji?*** Dały one podstawę do sformułowania hipotezy głównej, zakładającej, ***że obecny system informacyjny w organizacji publicznej na przykładzie uczelni wyższej nie w pełni chroni informację***. Występujące w środowisku uczelni wyższej zagrożenia bezpieczeństwa systemu

informacyjnego, wynikają z braku optymalnych zabezpieczeń informacji, niskiej świadomości użytkowników wspomnianego systemu, braku dodatkowych szkoleń tak potrzebnych przy wykonywaniu czynności związanych z użyciem systemu.

Negatywnym zjawiskiem, które zagraża bezpieczeństwu informacyjnemu jest także pomijanie przez użytkowników procedur bezpieczeństwa systemu informacyjnego w uczelni wyższej. Kluczową rolę w zapewnieniu bezpieczeństwa informacyjnego odgrywa otoczenie wewnętrzne i zewnętrzne uczelni wyższej powodem jest zróżnicowanie, mnogość użytkowników korzystających z tego systemu.

Pozyskane wyniki badań pokazują, że cel pracy został osiągnięty a problemy badawcze, które zostały sformułowane są rozwiązane. Potwierdzona została trafność przyjętych hipotez roboczych. Teraźniejsze czasy oparte są na cyfryzacji a wymaga to wzmożonej uwagi w obszarach bezpieczeństwa informacyjnego na zagrożenia. Postęp informacyjny umożliwia wdrożenie systemów posiadających wystarczające zabezpieczenia. Zabezpieczenia takie są bardzo ważne dla organizacji, ponieważ dane pozyskiwane i przetwarzane są pożądane przez grupy hackerskie. Zagrożenia bezpieczeństwa systemu informacyjnego mogą być minimalizowane poprzez poprawne kierunki implementacji zmian w obszarze organizacji uczelni wyższej
i zmiany zabezpieczeń systemu, które zostały szeroko omówione w czwartym rozdziale dysertacji. Nadzór i kontrola nad obiegiem informacji w organizacji publicznej powinna być wystarczająca, systematyczna i skuteczna.

Elementami decydującymi o skuteczności jest m.in. częstotliwość oraz dokładność ich przeprowadzania, a systematyczny wielopłaszczyznowy nadzór zwiększa bezpieczeństwo informacji będących w obiegu. Przeprowadzone badania dają możliwość wyciągnięcia wniosków stanowiących przedmiot badań i mieszczących się w katalogu zagrożeń. Należy zauważyć, że wśród osób badanych mała grupa osób posiada pełną świadomość o realnym stopniu zagrożenia dla bezpieczeństwa systemu informacyjnego w uczelni wyższej. W związku z powyższym należy w tym zakresie ukierunkować uczelnię na wdrożenie środków zaradczych.

Konieczny jest wpływ powodujący zwiększenie wiedzy wśród użytkowników systemu informacyjnego uczelni na temat jego zagrożeń jak również pełnego bezpieczeństwa a co najważniejsze jego podstawowej obsługi. Nowo przyjęte osoby powinny mieć zagwarantowane szkolenia systemowe w takiej ilości godzin, które pozwalałaby na swobodne działanie w systemie. Pozostali pracownicy powinny także przechodzić szkolenia okresowe związane z przypomnieniem zasad w zakresie działań w systemie jak również

zdobycie nowej wiedzy czy utrwalenie tej posiadanej. Uczelnia wyższa, aby zwiększyć poziom bezpieczeństwa potrzebuje zintegrowanego systemu, który połączy komórki występujące w organizacji w jedną spójną całość. Fakt ten będzie miał swoje przełożenie w sprawnym zarządzaniu organizacją.

Opracowana koncepcja bezpieczeństwa systemu informacyjnego pomagająca nakreślić nowe kierunki zmian w organizacji, jaką jest uczelnia wyższa w celu poprawy bezpieczeństwa systemu informacyjnego stworzy przesłanki do wdrożenia prac nad rozwiązaniami, które zostały zaproponowane i w domyśle mające mieć efektywne rozwiązania systemowe. W zakresie efektywnego zarządzania bezpieczeństwem powinny być wyznaczone dodatkowe osoby, mogące na bieżąco analizować poziom bezpieczeństwa systemu informacyjnego w uczelni wyższej. Taka potrzeba wynika z konieczności obsługi dużej społeczności akademickiej. Działania te zawierają, odbieranie sygnałów od użytkowników o zaistniałych problemach, incydentach, na które należy w szybki sposób reagować i wdrażać odpowiednie zabezpieczenia mające uchronić przed cyberprzestępczością.

BIBLIOGRAFIA

Ajdukiewicz K., *Logika pragmatyczna*, PWN, Warszawa 1965,

Ajdukiewicz K., *Zarys logiki*, PZWS, Warszawa 1956.

Aleksandrowicz T. R., *Podstawy walki informacyjnej*. *Bezpieczeństwo dziś i jutro,* EDO, Warszawa 2016.

Apanowicz J., *Metodologia nauk*, Dom Organizatora, Toruń 2003.

Balcerowicz B., *Siły zbrojne w stanie pokoju, kryzysu i wojny*, Wydawnictwo Naukowe Scholar, Warszawa 2010.

Bączek P., *Zagrożenia informacyjne a bezpieczeństwo państwa polskiego*, Wydawnictwo Adam Marszałek, Toruń 2006.

Bieniok H., *Metody sprawnego zarządzania. Planowanie, organizowanie, motywowanie, kontrola*, AW, Warszawa 1997.

Bryson B., *W domu,* Wydawnictwo Zysk i S-ka, Poznań 2010.

Ciborowski L., *Walka informacyjna*, Wydawnictwo Adam Marszałek, Toruń 2001.

Cieślarczyk M., Kuriata R., *Kryzys i sposoby radzenia sobie z nim,* Wydawnictwo Naukowe Wyższej Szkoły Kupieckiej, Łódź 2005.

Cieślarczyk M., *Metody, techniki i narzędzia badawcze oraz elementy statystyki stosowane w pracach magisterskich i doktorskich,* AON, Warszawa 2006.

Fehler W., *Zagrożenie – kluczowa kategoria teorii bezpieczeństwa, [w:] Współczesne postrzeganie bezpieczeństwa*, (red.) Jałoszyński K., Wiśniewski B., Wojtuszek T., WSA, Bielsko--Biała 2007.

Fertsch M., *Podstawy logistyki, Instytut Logistyki i Magazynowania*, Poznań 2006.

Flakiewicz W., *Systemy informacyjne w zarządzaniu. Uwarunkowania, technologie, rodzaje*, Wydawnictwo C. H. Beck, Warszawa 2012.

Forlicz S., *Informacje w biznesie*, PWE, Warszawa 2008.

Frankfort-Nachmias C., Nachmias D., *Metody badawcze w naukach społecznych,* Wydawnictwo Zysk i S-ka, Poznań 2001.

Fromm E., *Ucieczka od wolności,* Czytelnik, 1978.

Gibson W., *Neuromancer*, Poznań 1999.

Gierszewska G., Romanowska M., *Analiza strategiczna przedsiębiorstwa*, PWN, Warszawa 1997.

Giles K., *Handbook of Russian Information Warfare*, NATO 2016.

Goban-Klas T., Sienkiewicz P., *Społeczeństwo informacyjne – szanse, zagrożenia, wyzwania*, Wydawnictwo Fundacji Postępu Telekomunikacji, Kraków 1999.

Goliński M., *Społeczeństwo informacyjne - geneza koncepcji i problematyka pomiaru*, SGH - Oficyna Wydawnicza, Warszawa 2011

Hetmański M., *Świat informacji,* Difin, Warszawa 2015.
Hołyst B., *Wiktymologia*, PWN, Warszawa 1997.
Jakubczak W., *O stanie cyberbezpieczeństwa w Polsce–wybrane aspekty*, Przedsiębiorczość i Zarządzanie , 2016, 17 (5.1), 171-182
Jakubczak W., Gołębiowska A., Prokopowicz D., Jakubczak R., *Cybersecurity of Business Intelligence Analytics Based on the Processing of Large Sets of Information with the Use of Sentiment Analysis and Big Data*, European Research Studies Journal, 2021, 24 (4), 850-871
Janczak J., Nowak A., *Bezpieczeństwo informacyjne. Wybrane problemy, AON,* Warszawa 2013.
JP3-13 Joint Doctrine for Information Operations, Department of Defense, Washington 1998, [w:] T. R. Aleksandrowicz, *Podstawy walki informacyjnej*, Warszawa 2016.
Karatysz M., *Zjawisko cyberprzestępczości a polityka cyberbezpieczeństwa w regulacjach prawnych Rady Europy, Unii Europejskiej i Polski,* Wydawnictwo Naukowe UAM, Poznań 2013.
Karnowski M., Mistewicz E., *Anatomia władzy*, Wydawnictwo Czerwone i Czarne, Warszawa 2010.
Kędelski M., Roeske-Słomka I., *Statystyka*, AE Poznań, Poznań 1998.
Kolegowicz K., *Informacja w zarządzaniu przedsiębiorstwem*, (red.) Borowiecki R., Kwieciński M., Kantor Wydawniczy Zakamycze, Kraków 2003.
Komunikat Komisji Europa 2020. Strategia na rzecz inteligentnego i zrównoważonego rozwoju sprzyjającego włączeniu społecznemu, KE, Bruksela 2010.
Korzeniowski L. F., *Podstawy nauk o bezpieczeństwie,* Warszawa 2012.
Kotler P., *Marketing,* REBIS, Poznań 2005.
Kowalewski J., Kowalewski M., *Cyberterroryzm szczególnym zagrożeniem bezpieczeństwa państwa, „Telekomunikacja i techniki informacyjne*", 1-2/2014.
Kowalkowski S., *Niemilitarne zagrożenia bezpieczeństwa publicznego,* AON, Warszawa 2011.
Koziej S., *Teoria sztuki wojennej,* „Kwartalnik BELLONA", Warszawa 2011.
Kwećka R., *Informacja w walce zbrojnej,* AON, Warszawa 2001.
Leszczyńska M., *Współczesny model rozwoju społecznego z perspektywy rewolucji informacyjnej [w:] Nierówności społeczne a wzrost gospodarczy*. *Społeczeństwo informacyjne – regionalne aspekty rozwoju*, (red.) Woźniak M., UR, Rzeszów 2011.
Lewis J.A., *Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats,*
Liderman K., *Bezpieczeństwo informacyjne,* PWN, Warszawa 2012.
Liderman K., *Bezpieczeństwo informacyjne. Nowe wyzwania,* PWN, Warszawa 2017.
Liedel K., *Transsektorowe obszary bezpieczeństwa narodowego*, Difin, Warszawa 2011.
Liedel K., *Bezpieczeństwo informacyjne w dobie terrorystycznych i innych zagrożeń bezpieczeństwa narodowego*, Wydawnictwo Adam Marszałek, Toruń 2005.
Liedel K., Piasecka P., Aleksandrowicz T. R, *Analiza informacji. Teoria i praktyka zarządzanie bezpieczeństwem,* Difin, Warszawa 2012.

Liedel K., Serafin T., *Otwarte źródła informacji w działalności wywiadowczej,* Difin, Warszawa 2011.

Liedel K., *Zarządzanie informacją w walce z terroryzmem,* Wydawnictwo TRIO, Warszawa 2010.

Łobocki M., *Wprowadzenie do metodologii badań pedagogicznych*, Oficyna Wydawnicza Impuls, Kraków 2001.

Łobocki M., *Ustalania liczebności próby badawczej zobacz: Wprowadzenie do metodologii badań pedagogicznych, Oficyna Wydawnicza Impuls*, Warszawa 2010;

Pilch T., *Zasady badań pedagogicznych,* Żak Wydawnictwo Akademickie, Warszawa 1995;

Walasek-Jarosz B., *Tok realizacji badań oraz opracowanie wyników*, [w:] *Podstawy metodologii badań w pedagogice,* (red.) Palka S., GWP, Gdańsk 2010.

Łoś-Nowak T., *Bezpieczeństwo, [w:] Leksykon politologii*, (red.) Antoszewski A., Herbut R, Alta 2, Wrocław 2003.

Maciejewski M., *Prawo informacji – zagadnienia podstawowe, [w:] Prawo informacji. Prawo do informacji,* (red.) Góralczyk W., Wydawnictwo Wyższej Szkoły Przedsiębiorczości i Zarządzania im. Leona Koźmińskiego, Warszawa 2006.

Madej M., *Rewolucja informatyczna –istota, przejawy oraz wpływ na postrzeganie bezpieczeństwa państw i systemu międzynarodowego, [w:] Bezpieczeństwo teleinformatyczne państwa*, (red.) Madej M., Terlikowski M., Polski Instytut Spraw Międzynarodowych, Warszawa 2009.

Madej M., *Terroryzm i inne zagrożenia asymetryczne w świetle współczesnego pojmowania bezpieczeństwa narodowego i międzynarodowego – próba teoretycznej konceptualizacji, [w:] Porządek międzynarodowy u progu XXI wieku*, (red.) Kuźniar R., Wydawnictwo UW, Warszawa 2005.

Madej M., Terlikowski M., *Bezpieczeństwo teleinformatyczne państwa*, Polski Instytut Spraw Międzynarodowych, Warszawa 2009.

Majchrzak M., *Czy jest możliwe szkolne porozumiewanie się bez barier?, [w:] Czy polska szkoła ceni dobrą rozmowę? Komunikacja interpersonalna w edukacji,* (red.) Heller W., Poznań-Kalisz 2011.

Majchrzak M., *Wpływ rozwiązań informacyjnych na funkcjonowanie społeczeństwa, „Studia Kaliskie*", t. 7, 2019.

Majchrzak M., *Zarządzanie bezpieczeństwem informacyjnym,* [w:] Prakseologia w zarządzaniu i dowodzeniu. Racjonalność w zarządzaniu. Część 2, (red.) Kieżun W., Wołejszo J., Pisarska A., Kaliskie Towarzystwo Przyjaciół Nauk, Kalisz 2020.

Majchrzak M., *Sposoby przeprowadzania samooceny oraz prezentacja i wykorzystanie jej wyników w procesie zarządzania jednostką organizacyjną*, „Studia Kaliskie", t. 6, 2018.

Majchrzak M., *Effective Public Management in Local Government, „European Journal of Science and Research",* 1/2017.

Majewski T., Kurek D., *Dylematy kształcenia i doskonalenia oficerów w zakresie kompetencji przywódczych*, Wydawnictwo Uniwersytetu w Białymstoku, Białystok 2021
Majewski T., Kurek D., Szulc B.M., *Przywództwo, konteksty, reminiscencje*, ASzW, 2021
Maksimowicz-Ajchel A., *Wstęp do statystyki: Metody opisu statystycznego,* Wydawnictwo Uniwersytetu Warszawskiego, Warszawa 2007.
Mazur S., Ostrowska M., *Nowe kierunki w badaniach i naukach o edukacji w XXI wieku*, UKiP J&D Gębka, Kraków 2011
Mazur S., Bieniek M., *Bezpieczeństwo i obronność Rzeczypospolitej Polskiej*, Katowice 2006,
Mazur S. (red.), *Edukacja dla bezpieczeństwa*, Katowice 2006
Michalczewski G., *Czynniki kształtujące potrzeby informacyjne, [w:] Procesy informacyjne w obronności i bezpieczeństwie. Teoria i praktyka*, (red.) Wrzosek M., Wydawnictwo Akademii Sztuki Wojennej, Warszawa 2017.
Morańska D., *Szeroko Patologie w cyberprzestrzeni. Profilaktyka zagrożeń medialnych* Wydawnictwo Naukowe Wyższej Szkoły Biznesu, Dąbrowa Górnicza 2015.
Niezgoda M., *Społeczeństwo informacyjne w perspektywie socjologicznej: idea czy rzeczywistość?, [w:] Społeczeństwo informacyjne – wizja czy rzeczywistość,* (red.) Haber L., Uczelniane Wydawnictwo Naukowo-Dydaktyczne, Kraków 2003.
Nowak A., *Cyberprzestrzeń jako nowa jakość zagrożeń. Bezpieczeństwo Narodowe*, „Zeszyty Naukowe AON" nr 3(92), 2013, s. 5.
Nowak A., Scheffs W., *Zarządzanie bezpieczeństwem informacyjnym,* AON, Warszawa 2010.
Nowak E., Nowak M., *Zarys teorii bezpieczeństwa narodowego*, Difin, Warszawa 2011.
Overview OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security Polish translation, 2003.
Participant Obseryation and the CoUecfion and Interpretation of Data, „American Journal of Sociology", t. 40, 1955.
Pawłowski J., *Słownik terminów z zakresu bezpieczeństwa narodowego*, AON, Warszawa 2002.
Pelc M., *Wybrane problemy metodologiczne wojskowych badań naukowych, AON,* Warszawa 1998.
Pelc M., *Elementy metodologiczne badań naukowych.,* AON, Warszawa 2012.
Pilch T., Barman T., *Zasady badań pedagogicznych. Strategie jakościowe i ilościowe*, Żak Wydawnictwo Akademickie, Warszawa 2018.
Piwowarski J., *Transdyscyplinarna istota kultury bezpieczeństwa narodowego*, Wydawnictwo Naukowe Akademii Pomorskiej, Słupsk 2016.
Potejko P., *Bezpieczeństwo informacyjne, [w:] Bezpieczeństwo państwa*, (red.) Wojtaszczyk K.A., Materska-Sosnowska A., Oficyna Wydawnicza ASPRA-JR, Warszawa 2009.
Pułaska-Turyna B., *Statystyka dla ekonomistów,* Wydanie II rozszerzone, Difin, Warszawa 2008.
Pytkowski W., *Organizacja badań i ocena prac naukowych*, PWN, Warszawa 1985.

Reich L., Sawyer D., *Archiving Referencing Model*, White Book, Issue 5, CCSDS 19.

Schroeder M. J., *Spór o pojęcie informacji, „Studia Metodologiczne*", 2015/34.

Sekuła A., *Kryteria oceny ustaleń stanu faktycznego w audycie wewnętrznym*, Wydawnictwo Polskiego Instytutu Kontroli Wewnętrznej., Warszawa 2015.

Schwartau W., Information Warfare, New York 1994. Por.: P. Bączek, Zagrożenia informacyjne a bezpieczeństwo państwa polskiego, Wydawnictwo Adam Marszałek, Toruń 2005.

Sienkiewicz P, *Społeczeństwo informacyjne jako system cybernetyczny,* Uczelniane Wydawnictwo Naukowo-Dydaktyczne, Kraków 2004.

Sienkiewicz P., *Analiza systemowa rozwoju społeczeństwa informacyjnego, [w:] Rewolucja informacyjna i społeczeństwo,* (red.) Zacher L.W., Transformacje, Warszawa 1997.

Sienkiewicz P., *Teoria rozwoju społeczeństwa informacyjnego, [w:] Polskie doświadczenia w kształtowaniu społeczeństwa informacyjnego. Dylematy cywilizacyjno-kulturowe*, (red.) Haber L.H., Akademia Górniczo-Hutnicza, Kraków 2002, s. 506-507.

Słownik języka polskiego, PWN, Warszawa 1979.

Słownik łacińsko-polski w opracowaniu Kazimierza Kumanieckiego, PWN, Warszawa 1975.

Słownik współczesnego języka polskiego, Wydawnictwo Wilga, Warszawa 1996.

Sobczyk M., *Statystyka*, PWN, Warszawa 2007, s. 237.

Sobczyk M., *Statystyka*: Podstawy teoretyczne, przykłady, zadania, Wydawnictwo UMCS, Lublin 2000.

Soete L., *Building the Information Society for Ali Us. Finał Report of the High Level Export* Group (Bruksela: 1997) - wg [DÜKT2002].

Sutton R. J., *Bezpieczeństwo telekomunikacji,* przeł. G. Stawikowski, Wydawnictwo Komunikacji i Łączności, Warszawa 2004.

Szubrycht T., *Analiza podobieństw operacji militarnych innych niż wojna oraz działań pozwalających zminimalizowania zagrożenia asymetryczne*, „Zeszyty Naukowe Akademii Marynarki Wojennej", nr 1 (164), 2006.

Szubrycht T., *Cyberterroryzm jako nowa forma zagrożenia terrorystycznego*, „Zeszyty Naukowe Akademii Marynarki Wojennej", nr 1, 2005.

Tafoya W. L., Cyber Terror, „FBI Law Enforcement Bulletin", vol. 80, no. 11, 2011.

Walasek-Jarosz B., *Tok realizacji badań oraz opracowanie wyników*, [w:] *Podstawy metodologii badań w pedagogice*, (red.) Palka S., GWP, Gdańsk 2010, s. 177–199.

Wasilewski J., *Zarys definicji cyberprzestrzeni, [w:] Przegląd bezpieczeństwa narodowego*, (red.) Hołyst B., Wydawnictwo ABW, Warszawa 2013.

Wiśniewski E., *Metodyka wojskowych badań naukowych*, „Zeszyty Naukowe ASG WP" cz. 1(3), 1990.

Witkowska M., Cholawo-Soszoch K., *Społeczeństwo informacyjne. Istota, rozwój, wyzwania,* Wydawnictwo Akademickie i Profesjonalne, Warszawa 2006.

Wojciechowska-Filipek S., Ciekanowski Z., *Bezpieczeństwo informacyjne w cyberprzestrzeni jednostki - organizacji – państwa*, Wydawnictwo CeDeWu sp. z o.o., Warszawa 2016.

Wołejszo J., *Prakseologia w zarządzaniu i dowodzeniu*, „Studia Kaliskie", t. 2, 2014.

Wołejszo J., *System dowodzenia,* AON, Warszawa 2013.

Wołejszo J., *Organizacja pracy kierownika w organizacji zhierarchizowanej,* „Zeszyty Naukowe AON", nr 2(91), 2013.

Wołejszo J., Biernacik B., *Wsparcie informatyczne działań połączonych*, „Kwartalnik BELLONA" nr 2/2015 (681), Warszawa 2015.

Wołowski F., Zawiła Niedźwiecki J., *Bezpieczeństwo systemów informacyjnych. Praktyczny przewodnik zgodny z normami polskimi i międzynarodowymi*, Edu-Libri, Kraków-Warszawa 2012.

Wójcik J., *Kryminologiczne i kryminalistyczne problemy funkcjonowania wywiadu gospodarczego, [w:] System informacji strategicznej,* (red.) Borowiecki R., Romanowska M., Difin, Warszawa 2001.

Zięba R., *Instytucjonalizacja bezpieczeństwa europejskiego,* Wydawnictwo Scholar, Warszawa 1999.

Zięba R., *Bezpieczeństwo międzynarodowe po zimnej wojnie,* Wydawnictwa Akademickie i Profesjonalne, Warszawa 2008.

Żebrowski A, Kwiatkowski W., *Bezpieczeństwo informacji III Rzeczypospolitej*, Oficyna Wydawnicza ABRYS, Kraków 2000.

Netografia

Bangemann M., *Europa i społeczeństwo globalnej informacji. Zalecenia dla Rady Europejskiej,* Bruksela 1994 kbn.icm.edu.pl/gsi/raport.html [dostęp: 05.01.2024].

Biała Księga Bezpieczeństwa Narodowego RP, http://www.spbn.gov.pl/, [dostęp: 19.12.12.2022].

Denning D., *Testimony before the Special Oversight Panel on Terrorism Committee on Armed Services U.S. House of Representatives*, 2000, http://faculty.nps.edu/dedennin/publications/Testimony-Cyberterrorism2000.htm[(dostęp: 15.07.2022].

https://www.money.pl/__gospodarka/firmy-i-instytucje-placa-kary-za-wycieki-danych-jakie-to-kwoty-mamy-dane-6862541067500128a.html [dostęp: 4.11.2022].

http://wgospodarce.pl/informacje/57379-rozkreca-sie-afera-z-huawei[dostęp: 05.11.2022].

https://gloswielkopolski.pl/podlozone-bomby-na-poznanskich-uczelniach-rano-przyszly-emaile/ar/c1-15902903, [dostęp: 9.11.2023].

https://warszawa.naszemiasto.pl/alarmy-bombowe-na-polskich-uczelniach-studenci-donosza-o/ar/c1-8478401, [dostęp: 11.11.2023].

https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20180001668/U/D20181668Lj.pdf, [dostęp: 15.02.2022].
https://www.pka.edu.pl/2019/04/14/polska-komisja-akredytacyjna/,[dostęp: 19.11.2023].
https://zpe.gov.pl/a/cyberterroryzm/D4HRR86ro, [dostęp: 28.12.2023].
https://www.fakt.pl/wydarzenia/swiat/hakerzy-przejeli-rzadowa-strone-usa-groza-donaldowi-trumpowi/876len6, [dostęp: 02.01.2024].
https://www.tvp.info/46280362/cyberatak-wymierzony-w-wojska-usa-w-polsce-hakerzy-podszyli-sie-pod-znany-portal [dostęp: 02.01.2024].
https://www.computerworld.pl/news/Cyberbezpieczenstwo-wsrod-najwiekszych-ryzyk-biznesowych-w-2020- r,417286.html?utm_surce=news&utm_campaign=polecane&utm_medium=tags [dostęp: 25.012.2023].
https://leb.fbi.gov/2011/november/leb-november-2011 [dostęp:17.12.2023].
https://monitor.uksw.edu.pl/docs/download/2939287b3c61177a675bd574eeb16494,[dostęp:28.12.2023].
https://monitor.uksw.edu.pl/docs/download/2939287b3c61177a675bd574eeb16494,[dostęp:28.12.2023].
https://www.uken.krakow.pl/polityka-prywatnosci, [dostęp: 5.12.2024].
https://www.uken.krakow.pl/klauzula-rodo, [dostęp: 5.01.2024].
https://www.uken.krakow.pl/klauzula-rodo, [dostęp: 5.01.2024].
Janowski J., *Cyberkultura prawa. Współczesne problemy filozofii i informatyki prawa*, Warszawa 2012; Janowski J., Globalna cyberkultura polityki i prawa, http://www.bibliotekacyfrowa.pl/Content/46512/23_Jacek_Janowski.pdf, s. 316 i n. [dostęp: 24.10.22].
Center for Strategic & International Studies, 2002, s. 1, http://csis.org/files/media/csis/pubs/021101_risks_of_cyberterror.pdf [dostęp: 25.12.2023].
Ministerstwo Łączności Komitet Badań Naukowych, Raport: *Cele i kierunki rozwoju społeczeństwa informacyjnego w Polsce,* Warszawa, 28 listopada 2000 r. http://kbn.icm.edu.pl[dostęp: 25.05.22]
Pollit M. M., *Cyberterrorism – Fact or a Fancy?, [w:] Focus on Terrorism*, ed. E.V. Lin-den, New York 2007, s. 67, https://books.google.pl/books?id=wl=-D 42 sYMDIC&pg=P65 A&dq-Cyberterrorism+%E2%80%93+Fact+or+Fancy&hl=pl&sa=X&redir_esc=y#v=onepage&q=Cyberterrorism%20%E2%80%93%20Fact%20or%20Fancy&f=false [dostęp: 25.12.2023].
Rychły-Lipińska A., *Model bezpieczeństwa jednostki we współczesnym zmieniającym się otoczeniu – wstępne rozważania,* „Studia nad bezpieczeństwem", nr 2, 2017,http://cejsh.icm.edu.pl/cejsh/element/bwmeta1.element.desklightb3be4d04-9cf4-4281-9a41-1e502805c885 [dostęp:12.10.2022].

Sienkiewicz P., *Analiza systemowa zagrożeń dla bezpieczeństwa cyberprzestrzeni, „Automatyka*", t. 13 z 2, 2009, s. 589. http://journals.bg.agh.edu.pl/AUTOMATYKA/2009-02/Auto46.pdf [dostęp: 10.11.2022].
Wołejszo J., *Formy szkolenia obronnego w podsystemie niemilitarnym,* „ Studia Kaliskie" t. 6, 2018.
www.sjp.pwn.pl [dostęp: 1.12.2022].

Akty prawne

Konstytucja RP uchwalona w dniu 02 kwietnia 1997 r. przez Zgromadzenie Narodowe, przyjęta przez naród w referendum konstytucyjnym w dniu 25 maja 1997 r., podpisana przez Prezydenta Rzeczypospolitej Polskiej 16 lipca 1997 r., tekst ogłoszony (Dz. U. z 1997 r. nr 78 poz. 483).
Ustawa z 14 czerwca 1960 r. *Kodeks postępowania administracyjnego* (Dz. U. z 2020 r. poz. 256, 695, 1298).
Ustawa z dnia 20.07.2018 r., *Prawo o szkolnictwie wyższym i nauce* (Dz.U. z 2018 r., poz. 1668).
Ustawa z 10 maja 2018 r. *o ochronie danych osobowych* (Dz. U. 2018 r. poz. 1000).
Ustawa z dnia 27 lipca 2001 r. *o ochronie baz danych* (Dz. U. 2019 r. poz. 2134).
Ustawa z 05 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. 2019 r. poz. 742).
Ustawa z 29 września 1994 r. o rachunkowości (Dz. U. z 2019 r. poz. 351, 1495, 1571, 1655, 1680 z 2020 r. poz. 568).
Ustawa z dnia 27 sierpnia 2009 *o finansach publicznych*, Dz. U. z 2009, Nr 157, poz. 1240, art. 68.
Ustawa z 06 czerwca 1997 r. Kodeks karny wykonawczy (Dz. U. z 2020 r. poz. 523).
Ustawa z dnia 16 lipca 2004 r. prawo telekomunikacyjne (Dz. U. z 2019 r. poz. 2460, 2020 r. poz. 374, 695, 875).
Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. z 2020 r. poz. 344).
Ustawa z 29 września 1994 r. o rachunkowości (Dz. U. z 2019 r. poz. 351, 1495, 1571, 1655, 1680 z 2020 r. poz. 568).
Ustawa z dnia 05 września 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. 2020 r. poz. 1369).
Ustawa z dnia 20 lipca 2000 r. o ogłaszaniu aktów normatywnych i niektórych innych aktów prawnych (Dz. U. 2019 r., poz. 1461).
Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), (Dz. Urz. UEL119 z 04.05.2016 r., str.1, z późn. zm.).

Rozporządzenie Prezesa Rady Ministrów z 7 grudnia 2017 r. w sprawie przekazywania informacji, udostępniania dokumentów oraz udzielania pomocy służbom i instytucjom uprawnionym do prowadzenia poszerzonych postępowań sprawdzających, kontrolnych postępowań sprawdzających oraz postępowań bezpieczeństwa przemysłowego (Dz. U. 2017 r. poz. 2334).

Rozporządzenie Prezesa Rady Ministrów z 20 lipca 2011 r. w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego (Dz. U. 2011 r. nr 159 poz. 948).

RODO – Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UEL119 z 04.05.2016 r., str.1, z późn. zm.).

Polska Norma PN-EN ISO/IEC 27002:2017-06 – Technika informatyczna – Techniki bezpieczeństwa – Praktyczne zasady zabezpieczania informacji (Norma Międzynarodowa zawiera wytyczne związane z ustanowieniem, wdrożeniem, eksploatacją, monitorowaniem, przeglądem, utrzymaniem i doskonaleniem Systemu Zarządzania Bezpieczeństwem Informacji).

Polska Norma PN-EN ISO/IEC 27001:2017-06 – Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji – Wymagania (Norma Międzynarodowa określa wymagania dotyczące ustanowienia, wdrożenia, utrzymania i ciągłego doskonalenia systemu zarządzania bezpieczeństwem informacji w odniesieniu do organizacji. Niniejsza Norma Międzynarodowa obejmuje również wymagania dotyczące szacowania i postępowania z ryzykiem dotyczącym bezpieczeństwa informacji, dostosowanych do potrzeb organizacji. Wymogi określone w niniejszej Normie Międzynarodowej są ogólne i mają zastosowanie do wszystkich organizacji, niezależnie od typu, wielkości i charakteru. Wyłączenie któregokolwiek z wymagań określonych w Rozdziałach 4 do 10 jest nieakceptowalne, w wypadku gdy organizacja deklaruje zgodność z niniejszą Normą Międzynarodową).

Polska Norma PN-ISO/IEC 27006:2016-12 Technika informatyczna – Techniki bezpieczeństwa – Wymagania dla jednostek prowadzących audyt i certyfikację systemów zarządzania bezpieczeństwem informacji. (W Normie Międzynarodowej przedstawiono wymagania i podano wytyczne dla jednostek prowadzących audyt i certyfikację systemów zarządzania bezpieczeństwem informacji (SZBI) jako uzupełnienie wymagań zamieszczonych w ISO/IEC 17021 i ISO/IEC 27001. Głównym zamierzeniem jest pomoc w akredytacji jednostek certyfikujących prowadzących certyfikację SZBI. Wymagania podane w niniejszej Normie Międzynarodowej powinny być przedstawiane w kategoriach kompetencji i pewności przez każdą jednostkę prowadzącą certyfikację SZBI, a wytyczne zawarte w niniejszej Normie Międzynarodowej dostarczają dodatkowej interpretacji tych wymagań dla każdej jednostki prowadzącej certyfikację SZBI. Niniejsza Norma

Międzynarodowa, jako dokument zawierający kryteria, może być stosowana do akredytacji, oceny równorzędnej lub innych procesów audytowych)[1]

Polska Norma PN-ISO/IEC 27013:2014-01 – Technika informatyczna – Techniki bezpieczeństwa – Wytyczne do zintegrowanego wdrożenia ISO/IEC 27001 oraz ISO/IEC 20000-1 (W Normie Międzynarodowej podano wytyczne do zintegrowanego wdrożenia ISO/IEC 27001 oraz ISO/IEC 20000-1 dla tych organizacji, które zamierzają, wdrożyć ISO/IEC 27001 w sytuacji, gdy ISO/IEC 20000-1 (została wdrożona), wdrożyć obie normy ISO/IEC 27001 oraz ISO/IEC 20000-1 (równocześnie),zintegrować istniejące systemy zarządzania zgodne, odpowiednio, z ISO/IEC 27001 oraz ISO/IEC 20000-1. W niniejszej Normie Międzynarodowej skoncentrowano się wyłącznie na zintegrowanym wdrożeniu ISO/IEC 27001 oraz ISO/IEC 20000-1)[2].

Polska Norma PN-ISO/IEC 27005:2014-01 Technika informatyczna – Techniki bezpieczeństwa – Zarządzanie ryzykiem w bezpieczeństwie informacji (W Normie Międzynarodowej podano wytyczne dotyczące zarządzania ryzykiem w bezpieczeństwie informacji. W niniejszej Normie Międzynarodowej rozwinięto ogólne koncepcje określone w ISO/IEC 27001, opracowano ją w celu wsparcia satysfakcjonującego wdrożenia podejścia do bezpieczeństwa opartego na zarządzaniu ryzykiem. Znajomość koncepcji, modeli, procesów i terminologii podanych w ISO/IEC 27001 oraz ISO/IEC 27002 jest istotna dla zrozumienia niniejszej Normy Międzynarodowej. Niniejsza Norma Międzynarodowa ma zastosowanie do wszystkich typów organizacji (np. przedsiębiorstw, instytucji rządowych, organizacji non-profit), które zamierzają zarządzać ryzykiem, które może spowodować naruszenie bezpieczeństwa informacji w tych organizacjach.

[1].https://wiedza.pkn.pl/web/guest/wyszukiwarka-norm, [dostęp:15.02.2023].
[2] http://normy.ekoinfonet.pl/norma.php?id=76637, [dostęp.16.02.2023].

SPIS RYSUNKÓW

Rysunek.1.1. Etapy procesu badawczego 40
Rysunek 2.1. Proces obiegu informacji..... 56
Rysunek 2.2. Relacje pomiędzy elementami bezpieczeństwa 62
Rysunek 2.3. Bezpieczeństwo informacyjne w organizacji, elementy składowe..... 66
Rysunek 2.4. Cykl życia systemu bezpieczeństwa informacyjnego 68
Rysunek 2.5. Rodzaje działań związanych z wykonawstwem projektów systemów..... 69
Rysunek 2.6 Cykl życia systemu bezpieczeństwa informacyjnego 70
Rysunek 2.7. Otoczenie systemu informacji w organizacji..... 71
Rysunek 2.8. Otoczenie uczelni wyższej 84
Rysunek 2.9. System informacyjny funkcjonujący w uczelni wyższej 87
Rysunek 3.1. Podział zagrożeń informacyjnych 130
Rysunek 3.2. Wojna informacyjna z podziałem na cel i działanie..... 140
Rysunek 3.3. Możliwości płynące z wykorzystania ICT..... 144
Rysunek 3.4. Działania przyczyniające się do wywołania zagrożenia..... 146
Rysunek 3.5. Planuj-wykonuj-sprawdzaj-działaj (PDCA), wykorzystywany w procesach systemu zarządzania bezpieczeństwem informacji (SZBI) 148
Rysunek 3.6. Działania w zarzadzaniu bezpieczeństwem 149
Rysunek 3.7. Czynności w strategii zarządzania incydentami..... 150
Rysunek 4.1. Struktura organizacyjna uczelni wyższej i uprawnienia użytkowników do systemu – projekt 305
Rysunek 4.2. System informacyjny funkcjonujący w uczelni wyższej obecnie funkcjonujący i ze zmianą 306
Rysunek 4.3.Zintegrowany system przed i po zmianie..... 362
Rysunek 4.4. Elementy bezpieczeństwa systemu informacyjnego..... 369

SPIS TABEL

Tabela 1.1. Ilościowe zestawienie ankietowanych grup badanych pod względem płci 28
Tabela 1.2. Charakterystyka respondentów grupy nauczyciele akademiccy pod względem wykształcenia z podziałem na stopnie naukowe i tytuły naukowe..... 29
Tabela 1.3. Charakterystyka respondentów grupy nauczyciele akademiccy pod względem wykształcenia z podziałem na stopnie naukowe i tytuły naukowe (kadra badawczo-dydaktyczna, dydaktyczna) z podziałem na płeć 30
Tabela 1.4. Charakterystyka respondentów grupy nauczyciele akademiccy pod względem stażu pracy i płci 31
Tabela 1.5. Charakterystyka respondentów grupy kadra administracyjna 33
Tabela 1.6. Charakterystyka respondentów grupy kadra administracyjna 34
Tabela 1.7. Charakterystyka respondentów grupy kadra administracyjna 35
Tabela 1.8. Charakterystyka respondentów grupy studenci (różne kierunki) pod względem stopnia i formy realizacji studiów..... 36
Tabela 1.9. Charakterystyka respondentów grupy studentów (różne kierunki) pod względem formy i realizacji studiów z podziałem na płeć 37
Tabela 1.10. Charakterystyka respondentów z podziałem na wiek i płeć..... 38
Tabela 1.11. Przebieg procesu badawczego..... 41
Tabela.2.1. Odpowiedzi respondentów (nauczycieli akademickich i kadry administracyjnej) na temat najczęściej wykorzystanego kanału służącego do przekazywania informacji, jakim jest (wirtualna uczelnia, dziekanat10/USOS)..... 88
Tabela 2.2. Odpowiedzi respondentów grupy reprezentującej nauczycieli akademickich oraz grupy reprezentującej studentów (różnych kierunków) na temat najczęściej wykorzystywanego kanału przekazywania informacji, jakim jest 90
Tabela 2.3. Odpowiedzi respondentów grupy kadra administracyjna i grupy studenci na temat najczęściej wykorzystywanego kanału do przekazywania informacji, jakim jest..... 92
Tabela 2.4. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy kadra administracyjna na temat najczęściej wykorzystywanego kanału do przekazywania informacji, jakim są informacje na piśmie..... 95
Tabela 2.5. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy studentów (różnych kierunków) na temat najczęściej wykorzystywanego kanału do przekazywania informacji, jakim są informacje na piśmie 97
Tabela. 2.6. Odpowiedzi respondentów grupy kadra administracyjna i grupy studenci na temat najczęściej wykorzystywanego kanału do przekazywania informacji, jakim 99
Tabela 2.7. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy kadra administracyjna na temat najczęściej wykorzystywanego kanału do przekazywania informacji, jakim jest przekaz ustny..... 101
Tabela.2.8. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy studentów (różnych kierunków) na temat najczęściej wykorzystywanego kanału do przekazywania informacji, jakim jest przekaz ustny 103
Tabela 2.9. Odpowiedzi respondentów grupy kadra administracyjna i grupy studentów (różnych kierunków) na temat najczęściej wykorzystywanego kanału do przekazywania informacji, jakim jest przekaz ustny 105
Tabela 2.10. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy kadra administracyjna na temat najczęściej wykorzystywanego kanału do przekazywania informacji, jakim jest poczta elektroniczna 107

Tabela 2.11. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy studenci (różne roczniki) na temat najczęściej wykorzystywanego kanału do przekazywania informacji, jakim jest poczta elektroniczna *109*
Tabela 2.12. Odpowiedzi respondentów grupy kadra administracyjna i grupy studenci (różne roczniki) na temat najczęściej wykorzystywanego kanału do przekazywania informacji, jakim jest poczta elektroniczna *111*
Tabela 2.13. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy kadra administracyjna na temat najczęściej wykorzystywanego kanału do przekazywania informacji, jakim jest Aplikacja MsTeams *113*
Tabela 2.14. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy studentów (różne roczniki) na temat najczęściej wykorzystywanego kanału do przekazywania informacji, jakim jest Aplikacja MsTeams *115*
Tabela 2.15. Odpowiedzi respondentów grupy kadra administracyjna i grupy studentów (różne roczniki) na temat najczęściej wykorzystywanego kanału do przekazywania informacji, jakim jest Aplikacja MsTeams *117*
Tabela 2.16. Podział pod względem najczęściej wykorzystywanego kanału przekazywania informacji w uczelni wyższej *119*
Tabela 3.1. Odpowiedzi respondentów pracowników grupy nauczyciele akademiccy i grupy kadra administracyjna na temat zagrożeń systemu informacyjnego w szkole przez klęski żywiołowe, pożar *157*
Tabela. 3.2. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupa studenci (różne kierunki) na temat zagrożeń systemu informacyjnego w uczelni wyższej *159*
Tabela 3.3. Odpowiedzi respondentów pracowników grupy kadra administracyjna i grupa studenci (różne kierunki na temat zagrożeń systemu informacyjnego w uczelni wyższej przez klęski żywiołowe, pożar *161*
Tabela. 3.4. Odpowiedzi respondentów pracowników grupy nauczyciele akademiccy i grupa kadra administracyjna na temat zagrożeń systemu informacyjnego w uczelni wyższej przez utratę danych *163*
Tabela 3.5. Odpowiedzi respondentów pracowników grupy nauczyciele akademiccy i grupy studentów (różne kierunki) na temat zagrożeń systemu informacyjnego w uczelni wyższej przez utratę danych *165*
Tabela 3.6. Odpowiedzi respondentów pracowników grupy kadra administracyjna i grupy studentów (różne kierunki) na temat zagrożeń systemu informacyjnego w uczelni wyższej przez utratę danych *167*
Tabela 3.7. Odpowiedzi respondentów pracowników grupy nauczyciele akademiccy i grupy kadra administracyjna na temat zagrożeń systemu informacyjnego w uczelni wyższej przez zmianę hasła przez osoby trzecie i brak dostępu do własnego konta użytkownika *169*
Tabela 3.8. Odpowiedzi respondentów pracowników grupy nauczyciele akademiccy i grupy studenci (różne kierunki) na temat zagrożeń systemu informacyjnego w uczelni wyższej w wyniku zmiany hasła przez osoby trzecie i brak dostępu do własnego konta użytkownika *172*
Tabela 3.9. Odpowiedzi respondentów pracowników grupy kadra administracyjna i grupy studenci (różne kierunki) na temat zagrożeń systemu informacyjnego w uczelni wyższej w wyniku zmiany hasła przez osoby trzecie i brak dostępu do własnego konta użytkownika *174*
Tabela 3.10. Odpowiedzi respondentów pracowników nauczyciele akademiccy i grupy kadra naukowa na temat zagrożeń systemu informacyjnego w uczelni wyższej przez *177*
Tabela 3.11. Odpowiedzi respondentów pracowników nauczyciele akademiccy i grupy studenci (różne kierunki) na temat zagrożeń systemu informacyjnego w uczelni wyższej przez rozkodowanie hasła dostępu *179*

Tabela 3.12. Odpowiedzi respondentów pracowników kadry administracyjnej i grupy studenci (różne kierunki) na temat zagrożeń systemu informacyjnego w uczelni 181
Tabela 3.13. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy kadra administracyjna na temat zagrożeń systemu informacyjnego w uczelni wyższej 183
Tabela. 3.14. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy studenci (różne kierunki) na temat zagrożeń systemu informacyjnego w uczelni wyższej 185
Tabela 3.15. Odpowiedzi respondentów grupy kadra administracyjna i grupy studenci (różne kierunki) na temat zagrożeń systemu informacyjnego w uczelni wyższej 187
Tabela 3.16. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy kadra administracyjna na temat zagrożeń systemu informacyjnego w uczelni wyższej przez przekazywanie informacji osobom nieuprawnionym 189
Tabela 3.17. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy studenci (różne kierunki) na temat zagrożeń systemu informacyjnego w uczelni wyższej 192
Tabela 3.18. Odpowiedzi respondentów grupy kadra administracyjna i grupy studenci (różne kierunki) na temat zagrożeń systemu informacyjnego w uczelni wyższej przez przekazywanie informacji osobom nieuprawnionym..... 194
Tabela 3.19. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy kadra administracyjna na temat zagrożeń systemu informacyjnego w uczelni wyższej..... 196
Tabela 3.20. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy studenci (różne kierunki) na temat zagrożeń systemu informacyjnego w uczelni wyższej 198
Tabela 3.21. Odpowiedzi respondentów grupy kadra administracyjna i grupy studenci (różne kierunki) na temat zagrożeń systemu informacyjnego w uczelni wyższej 200
Tabela 3.22. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy kadra administracyjna na temat zagrożeń systemu informacyjnego w uczelni wyższej przez wykorzystywanie luk w zabezpieczeniach dostępu do poczty elektronicznej 202
Tabela 3.23. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy studenci (różne kierunki) na temat zagrożeń systemu informacyjnego w uczelni wyższej przez wykorzystanie luk w zabezpieczeniach do poczty elektronicznej i serwisu informacyjnego 204
Tabela 3.24. Odpowiedzi respondentów grupy kadra administracyjna i grupy studenci (różne kierunki) na temat zagrożeń systemu informacyjnego w uczelni wyższej przez wykorzystanie luk w zabezpieczeniach do poczty elektronicznej i serwisu informacyjnego 207
Tabela 3.25. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy kadra administracyjna na temat zagrożeń systemu informacyjnego w uczelni wyższej przez programy wykorzystujące błędy w systemach operacyjnych i w oprogramowaniu użytkowym 209
Tabela 3.26. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy studenci (różne kierunki) na temat zagrożeń systemu informacyjnego w uczelni wyższej przez programy wykorzystujące błędy w systemach operacyjnych i w oprogramowaniu użytkowym 211
Tabela 3.27. Odpowiedzi respondentów grupy kadra administracyjna i grupy studenci (różne kierunki) na temat zagrożeń systemu informacyjnego w uczelni wyższej przez programy wykorzystujące błędy w systemach operacyjnych i w oprogramowaniu użytkowym 213
Tabela 3.28. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy kadra administracyjna na temat zagrożeń systemu informacyjnego w uczelni wyższej..... 215
Tabela 3.29. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy studenci (różne kierunki)na temat stopnia zagrożenia systemu uczelni wyższej 217
Tabela 3.30. Odpowiedzi respondentów grupy kadra administracyjna i grupy studenci (różne kierunki) na temat zagrożeń systemu informacyjnego w uczelni wyższej 219
Tabela 3.31. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy kadra administracyjna na temat zagrożeń systemu informacyjnego w uczelni wyższej..... 221

Tabela 3.32. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy studenci (różne kierunki) na temat zagrożeń systemu informacyjnego w uczelni wyższej 223
Tabela 3.33. Odpowiedzi respondentów grupy kadra administracyjna i grupy studenci (różne kierunki) na temat zagrożeń systemu informacyjnego w uczelni wyższej przez obecność podejrzanego oprogramowania 225
Tabela 3.34. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy kadra administracyjna na temat zagrożeń systemu informacyjnego w uczelni wyższej przez manipulację danymi w systemie 227
Tabela 3.35. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy studenci (różne kierunki) na temat zagrożeń systemu informacyjnego w uczelni wyższej 229
Tabela 3.36. Odpowiedzi respondentów grupy kadra administracyjna i grupy studenci (różne kierunki) na temat zagrożeń systemu informacyjnego w uczelni wyższej 231
Tabela 3.37. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy kadra administracyjna na temat zagrożeń systemu informacyjnego w uczelni wyższej 233
Tabela 3.38. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy studenci (różne kierunki) na temat zagrożeń systemu informacyjnego w uczelni wyższej przez ujawnienie informacji podczas przesyłania 235
Tabela 3.39. Odpowiedzi respondentów grupy kadra administracyjna i grupy studenci (różne kierunki) na temat zagrożeń systemu informacyjnego w uczelni wyższej 237
Tabela 3.40. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy kadra administracyjna na temat stopnia zagrożenia systemu uczelni wyższej 239
Tabela 3.41. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy studentów (różne kierunki) na temat zagrożeń systemu informacyjnego w uczelni wyższej 241
Tabela 3.42. Odpowiedzi respondentów grupy kadra administracyjna i grupy studentów (różne kierunki) na temat zagrożeń systemu informacyjnego w uczelni wyższej 243
Tabela 3.43. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy kadra administracyjna na temat zagrożeń systemu informacyjnego w uczelni wyższej 245
Tabela 3.44. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy studenci (różne kierunki) na temat zagrożeń systemu informacyjnego w uczelni wyższej 247
Tabela 3.45. Odpowiedzi respondentów grupy kadra administracyjna i grupy studenci (różne kierunki) na temat zagrożeń systemu informacyjnego w uczelni wyższej 249
Tabela 3.46. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy kadra administracyjna na temat zagrożeń systemu informacyjnego w uczelni wyższej 251
Tabela 3.47. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy studenci (różne kierunki) na temat zagrożeń systemu informacyjnego w uczelni wyższej 253
Tabela 3.48. Odpowiedzi respondentów grupy kadra administracyjna i grupy studenci (różne kierunki) na temat zagrożeń systemu informacyjnego w uczelni wyższej 255
Tabela 3.49. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy kadra administracyjna na temat zagrożeń systemu informacyjnego w uczelni wyższej 257
Tabela 3.50. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy studenci (różne kierunki) na temat zagrożeń systemu informacyjnego w uczelni wyższej 259
Tabela 3.51. Odpowiedzi respondentów grupy kadra administracyjna i grupy studenci (różne kierunki) na temat zagrożeń systemu informacyjnego w uczelni wyższej 261
Tabela 3.52. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy kadra administracyjna na temat odbiorców informacji w uczelni wyższej 263
Tabela 3.53. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy studenci (różne kierunki) na temat odbiorców informacji w uczelni wyższej 265

Tabela 3.54. Odpowiedzi respondentów grupy kadra administracyjna i grupy studenci (różne kierunki) na temat odbiorców informacji w uczelni wyższej 267
Tabela 3.55. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy kadra administracyjna na temat braku dostępu do Internetu w uczelni wyższej 269
Tabela 3.56. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy studenci (różne kierunki) na temat braku dostępu do Internetu w uczelni wyższej 271
Tabela 3.57. Odpowiedzi respondentów grupy kadra administracyjna i grupy studenci (różne kierunki) na temat braku dostępu do Internetu w uczelni wyższej 273
Tabela 3.58. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy kadra administracyjna na temat problemów związanych z modernizacją 275
Tabela 3.59. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy studenci (różne kierunki) na temat problemów związanych z modernizacją 277
Tabela 3.60. Odpowiedzi respondentów grupy kadra administracyjna i grupy studenci (różne kierunki) na temat problemów związanych z modernizacją systemu 279
Tabela 3.61. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy kadra administracyjna na temat problemów związanych z awarią systemów w uczelni wyższej 281
Tabela 3.62. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy studenci (różne kierunki) na temat problemów związanych z awarią systemu 283
Tabela 3.63. Odpowiedzi respondentów grupy kadra administracyjna i grupy studenci (różne kierunki) na temat problemów związanych z awarią systemu 285
Tabela 3.64. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy kadra administracyjna na temat przestarzałego oprogramowania 287
Tabela 3.65. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy studenci (różne kierunki) na temat przestarzałego oprogramowania 289
Tabela 3.66. Odpowiedzi respondentów grupy kadra administracyjna i grupy studenci (różne kierunki) na temat przestarzałego oprogramowania 291
Tabela 3.67. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy kadra administracyjna na temat niewystarczającej ilości komputerów 293
Tabela 3.68. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy studenci (różne kierunki) na temat niewystarczającej ilości komputerów 295
Tabela 3.69. Odpowiedzi respondentów grupy kadra administracyjna i grupy studenci (różne kierunki) na temat niewystarczającej ilości komputerów 297
Tabela 4.1. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy kadra administracyjna na temat utrzymania w tajemnicy hasła dostępu do zasobów w sieci 307
Tabela 4.2. Odpowiedzi respondentów grupy nauczyciele akademiccy i studenci na temat utrzymania w tajemnicy hasła dostępu do zasobów w sieci 309
Tabela 4.3. Odpowiedzi respondentów grupy kadra administracyjna i grupy studenci (różne kierunki) na temat utrzymania w tajemnicy hasła dostępu do zasobów w sieci 311
Tabela 4.4. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy kadra administracyjna na temat zachowania bezpieczeństwa w posługiwaniu się 313
Tabela 4.5. Zaprezentowano rozkład odpowiedzi grupy nauczyciele akademiccy i grupy studenci (różne kierunki) na temat zachowania bezpieczeństwa w posługiwaniu się 315
Tabela 4.6. Odpowiedzi respondentów grupy kadra administracyjna i grupy studenci (różne kierunki) na temat zachowania bezpieczeństwa w posługiwaniu się 317
Tabela 4.7. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy kadra administracyjna na temat informowania administratora przez użytkowników uczelnianego systemu w przypadku utraty hasła lub podejrzenia, że zostało wykradzione i odczytane 320

Tabela 4.8. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy studenci (różne kierunki) na temat informowania administratora przez użytkowników szkolnego systemu w przypadku utraty hasła lub podejrzenia, ze zostało wykradzione *323*
Tabela 4.9. Odpowiedzi respondentów grupy kadra administracyjna i grupy studenci na temat informowania administratora przez użytkowników uczelnianego sytemu w przypadku utraty hasła lub podejrzenia, że zostało wykradzione *325*
Tabela 4.10. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy kadra administracyjna na temat sprawdzenia wiarygodności informacji odnośnie swojego ostatniego udanego logowania do systemu uczelni wyższej *328*
Tabela 4.11. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy studenci (różne kierunki) na temat sprawdzenia wiarygodności informacji odnośnie swojego ostatniego udanego logowania do systemu uczelni wyższej *330*
Tabela 4.12. Odpowiedzi respondentów grupy kadra administracyjna i grupy studenci (różne kierunki) na temat sprawdzania wiarygodności informacji odnośnie swojego ostatniego logowania do systemu uczelni wyższej *332*
Tabela 4.13. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy kadra administracyjna na temat osobistego informowania uczelnianego administratora odpowiedzialnego za system informacyjny o fakcie stwierdzenia nieścisłości *335*
Tabela 4.14. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy studenci (różne kierunki) na temat osobistego informowania uczelnianego administratora odpowiedzialnego za system informacyjny o fakcie stwierdzenia nieścisłości *337*
Tabela 4.15. Odpowiedzi respondentów grupy kadra administracyjna i grupy studenci (różne kierunki) na temat osobistego informowania uczelnianego administratora *339*
Tabela 4.16. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy kadra administracyjna na temat zachowania wszystkich zasad ochrony danych osobowych stosowanych w uczelni wyższej przez użytkowników w przypadku korzystania z prywatnego *342*
Tabela 4.17. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy studenci (różne kierunki) na temat zachowania wszystkich zasad ochrony danych osobowych stosowanych w uczelni wyższej przez użytkowników w przypadku korzystania z prywatnego komputera lub laptopa w dostępie do systemów wewnętrznych *344*
Tabela 4.18. Odpowiedzi respondentów grupy kadra administracyjna i grupy studenci (różne kierunki) na temat zachowania wszystkich zasad ochrony danych osobowych stosowanych w uczelni wyższej przez użytkowników w przypadku *346*
Tabela 4.19. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy kadra administracyjna na temat ujawnienia danych innym osobom w przypadku korzystania z prywatnego komputera/laptopa w dostępie do systemów wewnętrznych uczelni *349*
Tabela 4.20. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy studenci (różne kierunki) na temat ujawnienia danych osobom nieupoważnionym w przypadku korzystania z prywatnego komputera lub laptopa w dostępie *351*
Tabela 4.21. Odpowiedzi respondentów grupy kadra administracyjna i grupy studenci (różne kierunki) na temat ujawnienia danych osobom nieupoważnionym w przypadku korzystania z prywatnego komputera lub laptopa w dostępie *353*
Tabela 4.22. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy kadra administracyjna na temat zapoznania się przez nich z dostępnymi instrukcjami ułatwiającymi korzystanie z systemu informacyjnego w uczelni wyższej *355*
Tabela 4.23. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy studenci (różne kierunki) na temat zapoznania się przez nich z dostępnymi instrukcjami ułatwiającymi korzystanie z systemu informacyjnego w uczelni wyższej *357*

Tabela 4.24. Odpowiedzi respondentów grupy kadra administracyjna i grupy studenci (różne kierunki) na temat zapoznania się przez nich z dostępnymi instrukcjami ułatwiającymi korzystanie z systemu informacyjnego w uczelni wyższej 359
Tabela 4.25. Odpowiedzi respondentów grupy nauczyciele akademiccy, grupy kadra administracyjna na temat korzystania z konta indywidualnego, systemu informatycznego założonego każdemu pracownikowi uczelni/studentowi uczelni 363
Tabela 4.26. Odpowiedzi respondentów grupy nauczyciele akademiccy, grupy studenci (różne kierunki) na temat korzystania z konta indywidualnego, systemu informatycznego założonego każdemu pracownikowi uczelni/studentowi uczelni 365
Tabela 4.27. Odpowiedzi respondentów grupy kadra administracyjna, grupy studenci (różne kierunki) na temat korzystania z konta indywidualnego, systemu informatycznego założonego każdemu pracownikowi uczelni/studentowi uczelni 366
Tabela 4.28. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy kadra administracyjna na temat możliwości uzyskania większego poziomu bezpieczeństwa systemu informacyjnego w uczelni wyższej 370
Tabela 4.29. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy studenci (różne kierunki) na temat możliwości uzyskania większego poziomu bezpieczeństwa 373
Tabela 4.30. Odpowiedzi respondentów grupy kadra administracyjna i grupy studenci (różne kierunki) na temat możliwości uzyskania większego poziomu bezpieczeństwa systemu informacyjnego w uczelni wyższej 376
Tabela 4.31. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy kadra administracyjna na temat stopnia bezpieczeństwa systemu 379
Tabela 4.32. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy studenci (różne kierunki) na temat stopnia bezpieczeństwa systemu 381
Tabela 4.33. Odpowiedzi respondentów grupy kadra administracyjna i grupy studenci (różne kierunki) na temat stopnia bezpieczeństwa systemu 383

SPIS WYKRESÓW

Wykres 1.1. Ilościowe zestawienie ankietowanych grup badanych *29*
Wykres 1.2. Charakterystyka respondentów grupy nauczyciele akademiccy pod względem wykształcenia z podziałem na stopnie naukowe i tytuły naukowe..... *30*
Wykres 1.3. Charakterystyka respondentów grupy nauczyciele akademiccy pod względem wykształcenia z podziałem na stopnie naukowe i tytuły naukowe (kadra badawczo-dydaktyczna, dydaktyczna) z podziałem na płeć *31*
Wykres 1.4. Charakterystyka respondentów grupy nauczyciele akademiccy *32*
Wykres 1.5. Charakterystyka respondentów grupy kadra administracyjna..... *33*
Wykres 1.6. Charakterystyka respondentów grupy kadra administracyjna..... *34*
Wykres 1.7. Charakterystyka respondentów grupy kadra administracyjna..... *35*
Wykres 1.8. Charakterystyka respondentów grupy studenci (różne kierunki) pod względem stopnia i formy realizacji studiów *37*
Wykres 1.9. Charakterystyka respondentów grupy studentów (różne kierunki) pod względem formy i realizacji studiów z podziałem na płeć *38*
Wykres 1.10. Charakterystyka respondentów z podziałem na wiek i płeć *39*
Wykres 2.1. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy kadra administracyjna na temat najczęściej wykorzystywanego kanału służącego do przekazywania informacji, jakim jest (wirtualna uczelnia i dziekanat10/USOS)..... *89*
Wykres. 2.2. Zależności między respondentami, nauczycielami akademickimi i kadrą administracyjną pod względem najczęściej wykorzystywanego kanału do przekazywania informacji, jakim jest (wirtualna uczelnia i dziekanat10/USOS)..... *89*
Wykres 2.3. Odpowiedzi respondentów grupy nauczycieli akademickich i grupy studentów na temat najczęściej wykorzystanego kanału do przekazywania informacji, jakim jest (wirtualna uczelnia i dziekanat10/USOS)..... *91*
Wykres 2.4. Zależności między respondentami, nauczycielami akademickimi i studentami pod względem najczęściej wykorzystywanego kanału do przekazywania informacji, jakim jest (wirtualna uczelnia, dziekanat10/USOS)..... *92*
Wykres 2.5. Odpowiedzi respondentów grupy kadra administracyjna i grupy studenci na temat najczęściej wykorzystywanego kanału do przekazywania informacji, jakim jest..... *93*
Wykres 2.6. Zależność między respondentami grupy kadry administracyjnej i grupy studentów pod względem najczęściej wykorzystywanego kanału do przekazywania informacji, jakim jest (wirtualna uczelnia, dziekanat10/USOS)..... *94*
Wykres 2.7. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy kadra administracyjna na temat najczęściej wykorzystywanego kanału do przekazywania informacji, jakim są informacje na piśmie..... *96*
Wykres 2.8. Zależność między respondentami grupy nauczyciele akademiccy i grupy kadra administracyjna pod względem najczęściej wykorzystywanego kanału do przekazywania informacji, jakim są informacje na piśmie..... *96*
Wykres 2.9. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy studenci na temat najczęściej wykorzystywanego kanału do przekazywania informacji, ... *98*
Wykres 2.10. Zależność między respondentami grupy nauczyciele akademiccy i grupy studenci pod względem najczęściej wykorzystywanego kanału do przekazywania informacji, jakim są informacje na piśmie..... *98*
Wykres 2.11. Odpowiedzi respondentów pracowników administracyjnych i grupy studenci na temat najczęściej wykorzystywanego kanału do przekazywania informacji, jakim *100*

Wykres 2.12. Zależność między respondentami grupy kadra administracyjna i grupy studenci pod względem najczęściej wykorzystywanego kanału do przekazywania informacji, jakim są informacje na piśmie *101*
Wykres 2.13. Odpowiedzi respondentów pracowników grupy nauczycieli akademickich i grupy kadry administracyjnej na temat najczęściej wykorzystywanego kanału do przekazywania informacji, jakim jest przekaz ustny *102*
Wykres 2.14. Zależność między respondentami grupy nauczycieli akademickich i grupy kadry administracyjnej pod względem najczęściej wykorzystywanego kanału do przekazywania informacji, jakim jest przekaz ustny *103*
Wykres 2.15. Odpowiedzi respondentów pracowników grupy nauczycieli akademickich i grupy studentów (różnych roczników) na temat najczęściej wykorzystywanego kanału do przekazywania informacji, jakim jest przekaz ustny *104*
Wykres 2.16. Zależność między respondentami grupy nauczycieli akademickich i grupy studentów (różnych kierunków) pod względem najczęściej wykorzystywanego kanału do przekazywania informacji, jakim jest przekaz ustny *105*
Wykres 2.17. Odpowiedzi respondentów pracowników grupy kadra administracyjna i grupy studentów (różnych roczników) na temat najczęściej wykorzystywanego kanału do przekazywania informacji, jakim jest przekaz ustny *106*
Wykres 2.18. Zależność między respondentami grupy kadry administracyjnej i grupy studentów (różnych kierunków) pod względem najczęściej wykorzystywanego kanału do przekazywania informacji, jakim jest przekaz ustny *107*
Wykres 2.19. Odpowiedzi respondentów pracowników grupy nauczyciele akademiccy i grupy kadra administracyjna na temat najczęściej wykorzystywanego kanału do przekazywania informacji, jakim jest poczta elektroniczna *108*
Wykres 2.20. Zależność między respondentami grupy nauczycieli akademickich i grupy kadry administracyjnej pod względem najczęściej wykorzystywanego kanału do przekazywania informacji, jakim jest poczta elektroniczna *109*
Wykres 2.21. Odpowiedzi respondentów pracowników grupy nauczyciele akademiccy i grupy studenci (różnych roczników) na temat najczęściej wykorzystywanego kanału do przekazywania informacji, jakim jest poczta elektroniczna *110*
Wykres 2.22. Zależność między respondentami grupy nauczycieli akademickich i grupy studentów (różne roczniki) pod względem najczęściej wykorzystywanego kanału do przekazywania informacji, jakim jest poczta elektroniczna *111*
Wykres 2.23. Odpowiedzi respondentów pracowników kadra administracyjna i grupy studenci (różnych roczników) na temat najczęściej wykorzystywanego kanału do przekazywania informacji, jakim jest poczta elektroniczna *112*
Wykres 2.24. Zależność między respondentami grupy kadra administracyjna i grupy studentów (różne roczniki) pod względem najczęściej wykorzystywanego kanału do przekazywania informacji, jakim jest poczta elektroniczna *113*
Wykres 2.25. Odpowiedzi respondentów pracowników grupy nauczyciele akademiccy i grupy kadra administracyjna na temat najczęściej wykorzystywanego kanału do przekazywania informacji, jakim jest aplikacja MsTeams *114*
Wykres 2.26. Zależność między respondentami grupy nauczyciele akademiccy i grupy kadra administracyjna pod względem najczęściej wykorzystywanego kanału do przekazywania informacji, jakim jest aplikacja MsTeams *115*
Wykres 2.27. Odpowiedzi respondentów pracowników grupy nauczyciele akademiccy i grupy studentów (różnych roczników) na temat najczęściej wykorzystywanego kanału do przekazywania informacji, jakim jest aplikacja MsTeams *116*

Wykres 2.28. Zależność między respondentami grupy nauczyciele akademiccy i grupy studenci (różne roczniki) pod względem najczęściej wykorzystywanego kanału do przekazywania informacji, jakim jest aplikacja MsTeams 117
Wykres 2.29. Odpowiedzi respondentów pracowników grupy kadra administracyjna i grupy studentów (różnych roczników) na temat najczęściej wykorzystywanego kanału do przekazywania informacji, jakim jest aplikacja MsTeams 118
Wykres 2.30. Zależność między respondentami grupy kadra administracyjna i grupy studenci (różne roczniki) pod względem najczęściej wykorzystywanego kanału do przekazywania informacji, jakim jest aplikacja MsTeams 119
Wykres 2.31. Podziała pod względem najczęściej wykorzystywanego kanału przekazywania informacji w uczelni wyższej 120
Wykres 2.32. Ranking podziału pod względem najczęściej wykorzystywanego kanału przekazywania informacji w uczelni wyższej 120
Wykres 3.1. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy kadra naukowa na temat stopnia zagrożenia systemu uczelni wyższej 158
Wykres 3.2. Zależność między respondentami grupy nauczyciele akademiccy i grupy kadra administracyjna pod względem stopnia zagrożenia systemu uczelni wyższej 158
Wykres 3.3. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy studenci (różne kierunki) na temat stopnia zagrożenia systemu uczelni wyższej przez klęski żywiołowe, pożar 160
Wykres 3.4. Zależność między respondentami grupy nauczyciele akademiccy i grupy studenci (różne kierunki) pod względem stopnia zagrożenia systemu uczelni wyższej przez klęski żywiołowe, pożar 160
Wykres 3.5. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy studenci (różne kierunki) na temat stopnia zagrożenia systemu uczelni wyższej 162
Wykres 3.6. Zależność między respondentami grupy nauczyciele akademiccy i grupy studenci (różne kierunki) pod względem stopnia zagrożenia systemu uczelni wyższej 162
Wykres 3.7. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy kadra administracyjna na temat stopnia zagrożenia systemu uczelni wyższej przez utratę danych ... 164
Wykres 3.8. Zależność między respondentami grupy nauczyciele akademiccy i grupy kadra administracyjna pod względem stopnia zagrożenia systemu uczelni wyższej przez utratę danych 164
Wykres 3.9. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy studenci (różne kierunki) na temat stopnia zagrożenia systemu uczelni wyższej 166
Wykres 3.10. Zależność między respondentami grupy nauczyciele akademiccy i grupy studenci (różne kierunki) pod względem stopnia zagrożenia systemu uczelni wyższej 166
Wykres 3.11. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy studenci (różne kierunki) na temat stopnia zagrożenia systemu uczelni wyższej 168
Wykres 3.12. Zależność między respondentami grupy kadra administracyjna i grupy studenci (różne kierunki) pod względem stopnia zagrożenia systemu uczelni wyższej 169
Wykres 3.13. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy kadra administracyjna na temat stopnia zagrożenia systemu uczelni wyższej przez zmiany hasła przez osoby trzecie i brak dostępu do własnego konta użytkownika 170
Wykres 3.14. Zależność między respondentami grupy nauczyciele akademiccy i kadra administracyjna pod względem stopnia zagrożenia systemu uczelni wyższej w wyniku zmiany hasła przez osoby trzecie i brak dostępu do własnego konta użytkownika 171
Wykres 3.15. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy studenci (różne kierunki) na temat stopnia zagrożenia systemu uczelni wyższej w wyniku zmiany hasła przez osoby trzecie i brak dostępu do własnego konta użytkownika..... 173

Wykres 3.16. Zależność między respondentami grupy nauczyciele akademiccy i grupy studenci (różne kierunki) pod względem stopnia zagrożenia systemu uczelni wyższej w wyniku zmiany hasła przez osoby trzecie i brak dostępu do własnego konta użytkownika 174
Wykres 3.17. Odpowiedzi respondentów grupy kadra administracyjna i grupy studenci (różne kierunki) na temat stopnia zagrożenia systemu uczelni wyższej w wyniku zmiany hasła przez osoby trzecie i brak dostępu do własnego konta użytkownika..... 175
Wykres 3.18. Zależność między respondentami grupy kadra administracyjna i grupy studenci (różne kierunki) pod względem stopnia zagrożenia systemu uczelni wyższej w wyniku zmiany hasła przez osoby trzecie i brak dostępu do własnego konta użytkownika 176
Wykres 3.19. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy kadra administracyjna na temat stopnia zagrożenia systemu uczelni wyższej..... 177
Wykres 3.20. Zależność między respondentami grupy nauczyciele akademiccy i grupy kadra administracyjna pod względem stopnia zagrożenia systemu uczelni wyższej..... 178
Wykres 3.21. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy studenci (różne kierunki) na temat stopnia zagrożenia systemu uczelni wyższej 179
Wykres 3.22. Zależność między respondentami grupy nauczyciele akademiccy i grupy studenci (różne kierunki) pod względem stopnia zagrożenia systemu uczelni wyższej 180
Wykres 3.23. Odpowiedzi respondentów grupy kadra administracyjna i grupy studenci (różne kierunki) na temat stopnia zagrożenia systemu uczelni wyższej 182
Wykres 3.24. Zależność między respondentami grupy kadra administracyjna i grupy studenci (różne kierunki) pod względem stopnia zagrożenia systemu uczelni wyższej przez rozkodowanie hasła dostępu..... 183
Wykres 3.25. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy kadra administracyjna na temat stopnia zagrożenia systemu uczelni wyższej przez cyberatak..... 184
Wykres 3.26. Zależność między respondentami grupy nauczyciele akademiccy i grupy kadra administracyjna pod względem stopnia zagrożenia systemu uczelni wyższej..... 185
Wykres 3.27. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy studenci (różne kierunki) na temat stopnia zagrożenia systemu uczelni wyższej 186
Wykres 3.28. Zależność między respondentami grupy nauczyciele akademiccy i grupy studenci (różne kierunki) pod względem stopnia zagrożenia systemu uczelni wyższej 187
Wykres 3.29. Odpowiedzi respondentów grupy kadra administracyjna i grupy studenci (różne kierunki) na temat stopnia zagrożenia systemu uczelni wyższej 188
Wykres 3.30. Zależność między respondentami grupy kadra administracyjna i grupy studenci (różne kierunki) pod względem stopnia zagrożenia systemu uczelni wyższej 189
Wykres 3.31. Odpowiedzi respondentów grupy nauczyciele akademiccy i kadry administracyjnej na temat stopnia zagrożenia systemu uczelni wyższej przez przekazywanie informacji osobom nieuprawnionym..... 191
Wykres 3.32. Zależność między respondentami grupy nauczyciele akademiccy i grupy kadra administracyjna pod względem stopnia zagrożenia systemu uczelni wyższej..... 192
Wykres 3.33. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy studenci (różne kierunki) na temat stopnia zagrożenia systemu uczelni wyższej 193
Wykres 3.34. Zależność między respondentami grupy nauczyciele akademiccy i grupy studenci (różne kierunki) pod względem stopnia zagrożenia systemu uczelni wyższej 194
Wykres 3.35. Odpowiedzi respondentów grupy kadra administracyjna i grupy studenci (różne kierunki) na temat stopnia zagrożenia systemu uczelni wyższej przez przekazywanie informacji osobom nieuprawnionym 195
Wykres 3.36. Zależność między respondentami grupy kadra administracyjna i grupy studenci (różne kierunki) pod względem stopnia zagrożenia systemu uczelni wyższej 196

Wykres 3.37. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy kadra administracyjna na temat stopnia zagrożenia systemu uczelni wyższej *197*
Wykres 3.38. Zależność między respondentami grupy nauczyciele akademiccy i grupy kadra administracyjna pod względem stopnia zagrożenia systemu uczelni wyższej *198*
Wykres 3.39. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy studenci (różne kierunki) na temat stopnia zagrożenia systemu uczelni wyższej *199*
Wykres 3.40. Zależność między respondentami grupy nauczyciele akademiccy i grupy studenci (różne kierunki) pod względem stopnia zagrożenia systemu uczelni wyższej *200*
Wykres 3.41. Odpowiedzi respondentów grupy kadra administracyjna grupy studenci (różne kierunki) na temat stopnia zagrożenia systemu uczelni wyższej *201*
Wykres 3.42. Zależność między respondentami grupy kadra administracyjna i grupy studenci (różne kierunki) pod względem stopnia zagrożenia systemu uczelni wyższej *202*
Wykres 3.43. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy kadra administracyjna na temat stopnia zagrożenia systemu uczelni wyższej przez wykorzystanie luk w zabezpieczeniach do poczty elektronicznej i serwisu informacyjnego *203*
Wykres 3.44. Zależność między respondentami grupy nauczyciele akademiccy i grupy studenci (różne kierunki) pod względem stopnia zagrożenia systemu uczelni wyższej przez wykorzystanie luk w zabezpieczeniach do poczty elektronicznej i serwisu informacyjnego *204*
Wykres 3.45. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy studenci (różne kierunki) na temat stopnia zagrożenia systemu uczelni wyższej przez wykorzystanie luk w zabezpieczeniach do poczty elektronicznej i serwisu informacyjnego *205*
Wykres 3.46. Zależność między respondentami grupy nauczyciele akademiccy i grupy studenci (różne kierunki) pod względem stopnia zagrożenia systemu uczelni wyższej przez wykorzystanie luk w zabezpieczeniach do poczty elektronicznej *206*
Wykres 3.47. Odpowiedzi respondentów grupy kadra administracyjna i grupy studenci (różne kierunki) na temat stopnia zagrożenia systemu uczelni wyższej przez wykorzystanie luk w zabezpieczeniach do poczty elektronicznej i serwisu informacyjnego *208*
Wykres 3.48. Zależność między respondentami grupy kadra administracyjna i grupy studenci (różne kierunki) pod względem stopnia zagrożenia systemu uczelni wyższej przez wykorzystanie luk w zabezpieczeniach do poczty elektronicznej *208*
Wykres 3.49. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy kadra administracyjna na temat stopnia zagrożenia systemu uczelni wyższej przez wykorzystujące błędy w systemach operacyjnych i w oprogramowaniu użytkowym *210*
Wykres 3.50. Zależność między respondentami grupy nauczyciele akademiccy i grupy kadra administracyjna pod względem stopnia zagrożenia systemu uczelni wyższej przez programy wykorzystujące błędy w systemach operacyjnych i *211*
Wykres 3.51. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy studenci (różne kierunki) na temat stopnia zagrożenia systemu uczelni wyższej przez programy wykorzystujące błędy w systemach operacyjnych i w oprogramowaniu użytkowym *212*
Wykres 3.52. Zależność między respondentami grupy nauczyciele akademiccy i grupy studenci (różne kierunki) pod względem stopnia zagrożenia systemu uczelni wyższej przez programy wykorzystujące błędy w systemach operacyjnych i *213*
Wykres 3.53. Odpowiedzi respondentów grupy kadra administracyjna i grupy studenci (różne kierunki) na temat stopnia zagrożenia systemu uczelni wyższej przez programy wykorzystujące błędy w systemach operacyjnych i w oprogramowaniu użytkowym *214*
Wykres 3.54. Zależność między respondentami grupy kadra administracyjna i grupy studenci (różne kierunki) pod względem stopnia zagrożenia systemu uczelni wyższej przez programy wykorzystujące błędy w systemach operacyjnych *215*

Wykres 3.55. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy kadra administracyjna na temat stopnia zagrożenia systemu uczelni wyższej *216*
Wykres 3.56. Zależność między respondentami grupy nauczyciele akademiccy i grupy kadra administracyjna pod względem stopnia zagrożenia systemu uczelni wyższej *217*
Wykres 3.57. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy studenci (różne kierunki) na temat stopnia zagrożenia systemu uczelni wyższej *218*
Wykres 3.58. Zależności respondentów grupy nauczyciele akademiccy i grupy studenci (różne kierunki) na temat stopnia zagrożenia systemu uczelni wyższej *219*
Wykres 3.59. Odpowiedzi respondentów grupy kadra administracyjna i grupy studenci (różne kierunki) na temat stopnia zagrożenia systemu uczelni wyższej *220*
Wykres 3.60. Zależność między respondentami grupy kadra administracyjna i grupy studenci (różne kierunki) pod względem stopnia zagrożenia systemu uczelni wyższej *221*
Wykres 3.61. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy kadra administracyjna na temat stopnia zagrożenia systemu uczelni wyższej *222*
Wykres 3.62. Zależność między respondentami grupy nauczyciele akademiccy i grupy kadra administracyjna pod względem stopnia zagrożenia systemu uczelni wyższej *223*
Wykres 3.63. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy studenci (różne kierunki) na temat stopnia zagrożenia systemu uczelni wyższej *224*
Wykres 3.64. Zależność między respondentami grupy nauczyciele akademiccy i grupy studenci (różne kierunki) pod względem stopnia zagrożenia systemu uczelni wyższej *225*
Wykres 3.65. Odpowiedzi respondentów grupy kadra administracyjna i grupy studenci (różne kierunki) na temat stopnia zagrożenia systemu uczelni wyższej *226*
Wykres 3.66. Zależność między respondentami grupy kadry administracyjnej i grupy studenci (różne kierunki) pod względem stopnia zagrożenia systemu uczelni wyższej *227*
Wykres 3.67. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy kadra administracyjna na temat stopnia zagrożenia systemu uczelni wyższej *228*
Wykres 3.68. Zależność między respondentami grupy nauczyciele akademiccy i grupy kadra administracyjna pod względem stopnia zagrożenia systemu uczelni wyższej *229*
Wykres 3.69. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy studenci (różne kierunki) na temat stopnia zagrożenia systemu uczelni wyższej *230*
Wykres 3.70. Zależność między respondentami grupy nauczyciele akademiccy i grupy studenci (różne kierunki) pod względem stopnia zagrożenia systemu uczelni wyższej *231*
Wykres 3.71. Odpowiedzi respondentów grupy kadra administracyjna i grupy studenci (różne kierunki) na temat stopnia zagrożenia systemu uczelni wyższej *232*
Wykres 3.72. Zależność między respondentami grupy kadra administracyjna i grupy studenci (różne kierunki) pod względem stopnia zagrożenia systemu uczelni wyższej *233*
Wykres 3.73. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy kadra administracyjna na temat stopnia zagrożenia systemu uczelni wyższej *234*
Wykres 3.74. Zależność między respondentami grupy nauczyciele akademiccy i grupy kadra administracyjna pod względem stopnia zagrożenia systemu uczelni wyższej *235*
Wykres 3.75. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy studenci (różne kierunki) na temat stopnia zagrożenia systemu uczelni wyższej *236*
Wykres 3.76. Zależność między respondentami grupy nauczyciele akademiccy i grupy studenci (różne kierunki) pod względem stopnia zagrożenia systemu uczelni wyższej przez ujawnienie informacji podczas przesyłania *237*
Wykres 3.77. Odpowiedzi respondentów grupy kadra administracyjna i grupy studenci (różne kierunki) na temat stopnia zagrożenia systemu uczelni wyższej *238*

Wykres 3.78. Zależność między respondentami grupy kadra administracyjna i grupy studenci (różne kierunki) pod względem stopnia zagrożenia systemu uczelni wyższej 239
Wykres 3.79. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy kadra administracyjna na temat stopnia zagrożenia systemu uczelni wyższej 240
Wykres 3.80. Zależność między respondentami grupy nauczyciele akademiccy i grupy kadra administracyjna pod względem stopnia zagrożenia systemu uczelni wyższej 241
Wykres 3.81. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy studenci (różne kierunki) na temat stopnia zagrożenia systemu uczelni wyższej 242
Wykres 3.82. Zależność między respondentami grupy nauczyciele akademiccy i grupy studenci (różne kierunki) pod względem stopnia zagrożenia systemu uczelni wyższej przez podszywanie się pod inną osobę 243
Wykres 3.83. Odpowiedzi respondentów grupy kadra administracyjna i grupy studenci (różne kierunki) na temat stopnia zagrożenia systemu uczelni wyższej 244
Wykres 3.84. Zależność między respondentami grupy kadra administracyjna i grupy studenci (różne kierunki) pod względem stopnia zagrożenia systemu uczelni wyższej 245
Wykres 3.85. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy kadra administracyjna na temat stopnia zagrożenia systemu uczelni wyższej 246
Wykres 3.86. Zależność między respondentami grupy nauczyciele akademiccy i grupy kadra administracyjna pod względem stopnia zagrożenia systemu uczelni wyższej 247
Wykres 3.87. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy studenci (różne kierunki) na temat stopnia zagrożenia systemu uczelni wyższej 248
Wykres 3.88. Zależność między respondentami grupy nauczyciele akademiccy i grupy studenci (różne kierunki) pod względem stopnia zagrożenia systemu uczelni wyższej przez błędy, wady oprogramowania 249
Wykres 3.89. Odpowiedzi respondentów grupy kadra administracyjna i grupy studenci (różne kierunki) na temat stopnia zagrożenia systemu uczelni wyższej 250
Wykres 3.90. Zależność między respondentami grupy nauczyciele akademiccy i grupy studenci (różne kierunki) pod względem stopnia zagrożenia systemu uczelni wyższej 251
Wykres 3.91. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy kadra administracyjna na temat stopnia zagrożenia systemu uczelni wyższej 252
Wykres 3.92. Zależność między respondentami grupy nauczyciele akademiccy i kadra administracyjna pod względem stopnia zagrożenia systemu uczelni wyższej 253
Wykres 3.93. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy studenci (różne kierunki) na temat stopnia zagrożenia systemu uczelni wyższej 254
Wykres 3.94. Zależność między respondentami grupy nauczyciele akademiccy i grupy studenci (różne kierunki) pod względem stopnia zagrożenia systemu uczelni wyższej 255
Wykres 3.95. Odpowiedzi respondentów grupy kadra administracyjna i grupy studenci (różne kierunki) na temat stopnia zagrożenia systemu uczelni wyższej 256
Wykres 3.96. Zależność między respondentami grupy kadra administracyjna i grupy studenci (różne kierunki) pod względem stopnia zagrożenia systemu uczelni wyższej 257
Wykres 3.97. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy kadra administracyjna na temat stopnia zagrożenia systemu uczelni wyższej 258
Wykres 3.98. Zależność między respondentami grupy nauczyciele akademiccy i grupy kadra administracyjna pod względem stopnia zagrożenia systemu uczelni wyższej 259
Wykres 3.99. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy studenci (różne kierunki) na temat stopnia zagrożenia systemu uczelni wyższej 260
Wykres 3.100. Zależność między respondentami grupy nauczyciele akademiccy i grupy studenci (różne kierunki) pod względem stopnia zagrożenia systemu uczelni wyższej 261

Wykres 3.101. Odpowiedzi respondentów grupy kadra administracyjna i grupy studenci (różne kierunki) na temat stopnia zagrożenia systemu uczelni wyższej 262
Wykres 3.102. Zależność między respondentami grupy kadra administracyjna i grupy studenci (różne kierunki) pod względem stopnia zagrożenia systemu uczelni wyższej 263
Wykres 3.103. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy kadra administracyjna na temat najczęstszego odbiorcy informacji w systemie 264
Wykres 3.104. Zależność między respondentami grupy nauczyciele akademiccy i grupy kadra administracyjna temat odbiorców informacji w uczelni wyższej 265
Wykres 3.105. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy studenci (różne kierunki) na temat najczęstszego odbiorcy informacji w systemie..... 266
Wykres 3.106. Zależność między respondentami grupy nauczyciele akademiccy i grupy studenci (różne kierunki) na temat odbiorców informacji w uczelni wyższej..... 267
Wykres 3.107. Odpowiedzi respondentów grupy kadra administracyjna i grupy studenci (różne kierunki) na temat najczęstszego odbiorcy informacji w systemie..... 268
Wykres 3.108. Zależność między respondentami grupy kadra administracyjna i grupy studenci (różne kierunki) na temat odbiorców informacji w uczelni wyższej..... 269
Wykres 3.109. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy kadra administracyjna na temat braku dostępu do Internetu w uczelni wyższej..... 270
Wykres 3.110. Zależność między respondentami grupy nauczyciele akademiccy i grupy kadra administracyjna pod względem stopnia zagrożenia systemu uczelni wyższej..... 271
Wykres 3.111. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy studenci (różne kierunki) na temat stopnia zagrożenia systemu uczelni wyższej 272
Wykres 3.112. Zależność między respondentami grupy nauczyciele akademiccy i grupy studenci (różne kierunki) pod względem stopnia zagrożenia systemu uczelni wyższej 273
Wykres 3.113. Odpowiedzi respondentów grupy kadra administracyjna i grupy studenci (różne kierunki) na temat stopnia zagrożenia systemu uczelni wyższej 274
Wykres 3.114. Zależność między respondentami grupy kadra administracyjna i grupy studenci (różne kierunki) pod względem stopnia zagrożenia systemu uczelni wyższej 275
Wykres 3.115. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy kadra administracyjna na temat stopnia zagrożenia systemu uczelni wyższej..... 276
Wykres 3.116. Zależność między respondentami grupy nauczyciele akademiccy i grupy kadra administracyjna pod względem stopnia zagrożenia systemu uczelni wyższej..... 277
Wykres 3.117. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy studenci (różne kierunki) na temat stopnia zagrożenia systemu uczelni wyższej 278
Wykres 3.118. Zależność między respondentami grupy nauczyciele akademiccy i grupy studenci (różne kierunki) pod względem stopnia zagrożenia systemu uczelni wyższej 279
Wykres 3.119. Odpowiedzi respondentów grupy kadra administracyjna i grupy studenci (różne kierunki) na temat stopnia zagrożenia systemu uczelni wyższej 280
Wykres 3.120 Zależność między respondentami grupy kadra administracyjna i grupy studenci (różne kierunki) pod względem stopnia zagrożenia systemu uczelni wyższej przez modernizację systemu..... 281
Wykres 3.121. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy kadra administracyjna na temat stopnia zagrożenia systemu uczelni wyższej..... 282
Wykres 122. Zależność między respondentami grupy nauczyciele akademiccy i grupy kadra administracyjna pod względem stopnia zagrożenia systemu uczelni wyższej..... 283
Wykres 3.123. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy studenci (różne kierunki) na temat stopnia zagrożenia systemu uczelni wyższej 284

Wykres 3.124. Zależność między respondentami grupy nauczyciele akademiccy i grupy studenci (różne kierunki) pod względem stopnia zagrożenia systemu uczelni wyższej 285
Wykres 3.125. Odpowiedzi respondentów grupy kadra administracyjna i grupy studenci (różne kierunki) na temat stopnia zagrożenia systemu uczelni wyższej 286
Wykres 3.126. Zależność między respondentami grupy kadra administracyjna i grupy studenci (różne kierunki) pod względem stopnia zagrożenia systemu uczelni wyższej 287
Wykres 3.127. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy kadra administracyjna na temat stopnia zagrożenia systemu uczelni wyższej 288
Wykres 3.128. Zależność między respondentami grupy nauczyciele akademiccy i grupy kadry administracyjnej pod względem stopnia zagrożenia systemu uczelni wyższej 289
Wykres 3.129. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy studenci (różne kierunki) na temat stopnia zagrożenia systemu uczelni wyższej 290
Wykres 3.130. Zależność między respondentami grupy nauczyciele akademiccy i grupy studenci (różne kierunki) pod względem stopnia zagrożenia systemu uczelni wyższej 291
Wykres 3.131. Odpowiedzi respondentów grupy kadra administracyjna i grupy studenci (różne kierunki) na temat stopnia zagrożenia systemu uczelni wyższej 292
Wykres 3.132. Zależność między respondentami grupy kadra administracyjna i grupy studenci (różne kierunki) pod względem stopnia zagrożenia systemu uczelni wyższej 293
Wykres 3.133. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy kadra administracyjna na temat stopnia zagrożenia systemu uczelni wyższej 294
Wykres 3.134. Zależność między respondentami grupy nauczyciele akademiccy i grupy kadra administracyjna pod względem stopnia zagrożenia systemu uczelni wyższej 295
Wykres 3.135. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy studenci (różne kierunki) na temat stopnia zagrożenia systemu uczelni wyższej 296
Wykres 3.136. Zależność między respondentami grupy nauczyciele akademiccy i grupy studenci (różne kierunki) pod względem stopnia zagrożenia systemu uczelni wyższej 297
Wykres 3.137. Odpowiedzi respondentów grupy kadra administracyjna i grupy studenci (różne kierunki) na temat stopnia zagrożenia systemu uczelni wyższej 298
Wykres 3.138. Zależność między respondentami grupy kadra administracyjna i grupy studenci (różne kierunki) pod względem stopnia zagrożenia systemu uczelni wyższej 299
Wykres 4.1. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy kadra administracyjna na temat utrzymania w tajemnicy hasła dostępu do zasobów sieci 308
Wykres 4.2. Zależność miedzy respondentami grupy nauczyciele akademiccy i grupy kadra administracyjna pod względem utrzymywania w tajemnicy hasła dostępu 308
Wykres 4.3. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy studenci na temat utrzymywania w tajemnicy hasła dostępu do zasobów w sieci 309
Wykres 4.4. Zależności miedzy respondentami grupy nauczyciele akademiccy i grupy studenci różne kierunki pod względem utrzymania w tajemnicy hasła 310
Wykres 4.5. Odpowiedzi respondentów grupy kadra administracyjna i grupy studenci (różne kierunki) na temat utrzymania w tajemnicy hasła dostępu do zasobów w sieci 311
Wykres 4.6. Zależność między respondentami grupy kadra administracyjna i grupy studenci (różne kierunki) pod względem utrzymywania w tajemnicy hasła dostępu do zasobów w sieci 312
Wykres 4.7. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy kadra administracyjna na temat zachowania bezpieczeństwa w posługiwaniu się loginem 314
Wykres 4.8. Zależność między respondentami grupy nauczyciele akademiccy i grupy kadra administracyjna pod względem zachowania bezpieczeństwa w posługiwaniu się 315
Wykres 4.9. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy studenci (różne kierunki) na temat zachowania bezpieczeństwa w posługiwaniu się 316

Wykres 4.10. Zależność miedzy respondentami grupy nauczyciele akademiccy i grupy studenci (różne kierunki) pod względem zachowania bezpieczeństwa w posługiwaniu się loginem i hasłem do systemu *317*
Wykres 4.11. Odpowiedzi respondentów grupy kadra administracyjna i grupy studenci (różne kierunki) na temat zachowania bezpieczeństwa w posługiwaniu się *318*
Wykres 4.12. Zależność między respondentami grupy kadra administracyjna i grupy studenci (różne kierunki) pod względem zachowania bezpieczeństwa w posługiwaniu się loginem i hasłem do systemu *318*
Wykres 4.13. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy kadra administracyjna na temat informowania administratora przez użytkowników uczelnianego sytemu w przypadku utraty hasła lub podejrzenia, że zostało wykradzione i odczytane *321*
Wykres 4.14. Zależności między respondentami grupy nauczyciele akademiccy i grupy kadra administracyjna pod względem informowania administratora przez użytkowników uczelnianego sytemu w przypadku utraty hasła lub podejrzenia, ze zostało wykradzione i *322*
Wykres 4.15. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy studenci (różne kierunki) na temat informowania administratora przez użytkowników szkolnego systemu w przypadku utraty hasła lub podejrzenia, ze zostało wykradzione *323*
Wykres 4.16. Zależności pomiędzy respondentami grupy nauczyciele akademiccy i grupy studenci (różne kierunki) pod względem informowania administratora przez użytkowników uczelnianego systemu w przypadku utraty hasła lub podejrzenia, ze zostało wykradzione i odczytane przez osobę nieuprawniona *324*
Wykres 4.17. Odpowiedzi respondentów grupy kadra administracyjna i grupy studenci (różne kierunki) na temat informowania administratora przez użytkowników uczelnianego sytemu w przypadku utraty hasła lub podejrzenia, że zostało wykradzione *325*
Wykres 4.18 Zależności między respondentami grupy kadra administracyjna i grupy studenci (różne kierunki) pod względem informowania administratora przez użytkowników uczelnianego systemu w przypadku utraty hasła lub podejrzenia, ze zostało wykradzione i odczytane przez osobę nieuprawnioną *326*
Wykres 4.19. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy kadra administracyjna na temat sprawdzenia wiarygodności informacji odnośnie swojego ostatniego udanego logowania do sytemu uczelni wyższej *329*
Wykres 4.20. Zależność między respondentami grupy nauczyciele akademiccy i grupy kadra administracyjna pod względem sprawdzania wiarygodności informacji odnośnie swojego ostatniego udanego logowania do systemu uczelni wyższej *330*
Wykres 4.21. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy studenci (różne kierunki) na temat sprawdzania wiarygodności informacji odnośnie swojego ostatniego udanego logowania do systemu w uczelni wyższej *331*
Wykres 4.22. Zależność między respondentami grupy nauczyciele akademiccy i grupy studenci (różne kierunki) pod względem sprawdzenia wiarygodności informacji odnośnie swojego udanego logowania do systemu w uczelni wyższej *332*
Wykres 4.23. Odpowiedzi respondentów grupa kadra administracyjna i grupy studenci (różne kierunki) na temat sprawdzenia wiarygodności informacji odnośnie swojego ostatniego udanego logowania do systemu w uczelni wyższej *333*
Wykres 4.24. Zależność między respondentami grupy kadra administracyjna i grupy studenci (różne kierunki) pod względem sprawdzania wiarygodności informacji odnośnie swojego ostatniego udanego logowania do systemu w uczelni wyższej *334*

Wykres 4.25. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy kadra administracyjna na temat osobistego informowania uczelnianego administratora odpowiedzialnego za system informacyjny o fakcie stwierdzenia nieścisłości 336
Wykres 4.26. Zależność miedzy respondentami grupy nauczyciele akademiccy i grupy kadra administracyjna pod względem osobistego informowania uczelnianego administratora odpowiedzialnego za system informacyjny o fakcie stwierdzenia nieścisłości 337
Wykres 4.27. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy studenci (różne kierunki) na temat osobistego informowania uczelnianego administratora odpowiedzialnego za system informacyjny o fakcie stwierdzenia nieścisłości 338
Wykres 4.28. Zależność między respondentami grupy nauczyciele akademiccy i grupy studenci (różne kierunki) pod względem osobistego informowania uczelnianego 339
Wykres 4.29. Odpowiedzi respondentów grupy kadra administracyjna i grupy studenci (różne kierunki) na temat osobistego informowania uczelnianego administratora 340
Wykres 4.30. Zależność między respondentami grupy kadra administracyjna i grupy studenci (różne kierunki) na temat osobistego informowania uczelnianego administratora odpowiedzialnego za system informacyjny o fakcie stwierdzenia nieścisłości 341
Wykres 4.31. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy kadra administracyjna na temat zachowania wszystkich zasad ochrony danych osobowych stosowanych w uczelni wyższej przez użytkowników w przypadku korzystania z prywatnego komputera lub laptopa w dostępie do systemów wewnętrznych 343
Wykres 4.32. Zależność między respondentami grupy nauczyciele akademiccy i grupy kadra administracyjna pod względem zachowania wszystkich zasad ochrony danych osobowych stosowanych w uczelni wyższej przez użytkowników w przypadku korzystania z prywatnego komputera lub laptopa w dostępie do systemów wewnętrznych 343
Wykres 4.33 Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy studenci (różne kierunki) na temat zachowania wszystkich zasad ochrony danych osobowych stosowanych w uczelni wyższej przez użytkowników w przypadku korzystania z prywatnego komputera lub laptopa w dostępie do systemów wewnętrznych 345
Wykres 4.34. Zależność między respondentami grupy nauczyciele akademiccy i grupy studenci (różne kierunki) pod względem zachowania wszystkich zasad ochrony danych osobowych stosowanych w uczelni wyższej przez użytkowników w przypadku korzystania z prywatnego komputera lub laptopa w dostępie do systemów wewnętrznych 345
Wykres 4.35. odpowiedzi respondentów grupy kadra administracyjna i grupy studenci (różne kierunki) na temat zachowania wszystkich zasad ochrony danych osobowych stosowanych w uczelni wyższej przez użytkowników w przypadku korzystania z prywatnego komputera lub laptopa w dostępie do systemów wewnętrznych 347
Wykres 4.36. Zależność między respondentami grupy kadra administracyjna i grupy studenci (różne kierunki) pod względem zachowania wszystkich zasad ochrony danych osobowych stosowanych w uczelni wyższej przez użytkowników w przypadku korzystania z prywatnego komputera lub laptopa w dostępie do systemów wewnętrznych 347
Wykres 4.37. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy kadra administracyjna na temat ujawnienia danych osobom nieupoważnionym w przypadku korzystania z prywatnego komputera lub laptopa w dostępie 349
Wykres 4.38. Zależność między respondentami grupy nauczyciele akademiccy i grupy kadra administracyjna pod względem ujawnienia danych osobom nieupoważnionym w przypadku korzystania z prywatnego komputera lub laptopa w dostępie do systemów wewnętrznych uczelni 350

Wykres 4.39. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy studenci (różne kierunki) na temat ujawnienia danych osobom nieupoważnionym w przypadku korzystania z prywatnego komputera/laptopa w dostępie 351
Wykres 4.40. Zależność między respondentami grupy nauczyciele akademiccy i grupy studenci (różne kierunki) pod względem ujawnienia danych osobom nieupoważnionym w przypadku korzystania z prywatnego komputera/laptopa w dostępie..... 352
Wykres 4.41. Odpowiedzi respondentów grupy kadra administracyjna i grupy studenci (różne kierunki) na temat ujawnienia danych osobom nieupoważnionym w przypadku korzystania z prywatnego komputera/laptopa w dostępie do systemów wewnętrznych uczelni 353
Wykres 4.42. Zależność między respondentami grupy kadra administracyjna i grupy studenci (różne kierunki)) pod względem ujawnienia danych osobom nieupoważnionym w przypadku korzystania z prywatnego komputera/laptopa w dostępie..... 354
Wykres 4.43. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy kadra administracyjna na temat zapoznania się przez nich z dostępnymi instrukcjami ułatwiającymi korzystanie z systemu informacyjnego w uczelni wyższej 356
Wykres 4.44. Zależność między grupą nauczyciele akademiccy i grupą kadra administracyjna pod zapoznania się przez nich z dostępnymi instrukcjami ułatwiającymi korzystanie z systemu informacyjnego w uczelni wyższej..... 357
Wykres 4.45. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy studenci (różne kierunki) na temat zapoznania się przez nich z dostępnymi instrukcjami ułatwiającymi korzystanie z systemu informacyjnego w uczelni wyższej 358
Wykres 4.46. Zależność między grupą nauczyciele akademiccy i studenci (różne kierunki) pod względem zapoznania się przez nich z dostępnymi instrukcjami ułatwiającymi korzystanie z systemu informacyjnego w uczelni wyższej 359
Wykres 4.47. Odpowiedzi respondentów grupy kadra administracyjna i grupy studenci (różne kierunki) na temat zapoznania się przez nich z dostępnymi instrukcjami ułatwiającymi korzystanie z systemu informacyjnego w uczelni wyższej 360
Wykres 4.48. Zależność między grupą kadra administracyjna i studenci (różne kierunki) pod względem zapoznania się przez nich z dostępnymi instrukcjami ułatwiającymi korzystanie z systemu informacyjnego w uczelni wyższej..... 360
Wykres 4.49. Odpowiedzi respondentów grupy nauczyciele akademiccy, grupy kadra administracyjna na temat korzystania z konta indywidualnego, systemu informatycznego założonego każdemu pracownikowi uczelni/studentowi uczelni 364
Wykres 4.50.Zależnosci pomiędzy respondentami grupy nauczyciele akademiccy, grupy kadra administracyjna na temat korzystania z konta indywidualnego, systemu informatycznego założonego każdemu pracownikowi uczelni/studentowi uczelni..... 364
Wykres 4.51. Odpowiedzi respondentów grupy nauczyciele akademiccy, grupy studenci (różne kierunki) na temat korzystania z konta indywidualnego, systemu informatycznego założonego każdemu pracownikowi uczelni/studentowi uczelni..... 365
Wykres 4.52. Zależności pomiędzy respondentami grupy nauczyciele akademiccy, grupy studenci (różne kierunki) na temat korzystania z konta indywidualnego, systemu informatycznego założonego każdemu pracownikowi uczelni/studentowi uczelni 366
Wykres 4.53. Odpowiedzi respondentów grupy kadra administracyjna, grupy studenci (różne kierunki) na temat korzystania z konta indywidualnego, systemu informatycznego założonego każdemu pracownikowi uczelni/studentowi uczelni 367
Wykres 4.54. Zależności pomiędzy respondentami grupy kadra administracyjna, grupy studenci (różne kierunki) na temat korzystania z konta indywidualnego, systemu informatycznego założonego każdemu pracownikowi uczelni/studentowi uczelni 368

Wykres 4.55. Odpowiedzi respondentów grupy nauczyciele akademiccy na temat możliwości uzyskania większego poziomu bezpieczeństwa systemu 372
Wykres 4.56. Odpowiedzi respondentów grupy kadra administracyjna na temat możliwości uzyskania większego poziomu bezpieczeństwa systemu 373
Wykres 4.57. Odpowiedzi respondentów grupy studenci (różne kierunki) na temat możliwości uzyskania większego poziomu bezpieczeństwa systemu 375
Wykres 4.58. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy kadra administracyjna na temat stopnia bezpieczeństwa systemu 380
Wykres 4.59. Zależność między respondentami grupy nauczyciele akademiccy i grupy kadra administracyjna pod względem stopnia bezpieczeństwa systemu 380
Wykres 4.60. Odpowiedzi respondentów grupy nauczyciele akademiccy i grupy studenci (różne kierunki) na temat stopnia bezpieczeństwa systemu 382
Wykres 4.61. Zależność między respondentami grupy nauczyciele akademiccy i grupy studenci (różne kierunki) pod względem stopnia bezpieczeństwa systemu 382
Wykres 4. 62. Odpowiedzi respondentów grupy kadra administracyjna i grupy studenci (różne kierunki) na temat stopnia bezpieczeństwa systemu 383
Wykres 4.63. Zależność między respondentami grupy kadra administracyjna i grupy studenci (różne kierunki) pod względem stopnia bezpieczeństwa systemu 384

Wykaz załączników

Załącznik 1. Kwestionariusz ankiety i rozkład odpowiedzi

Załącznik 2. Kwestionariusz wywiadu eksperckiego ze sprawozdaniem

Złącznik 3. Arkusz obserwacji

Załącznik 1

KWESTIONARIUSZ ANKIETY

- *NAUCZYCIELE AKADEMICCY*
- *KADRA ADMINISTRACYJNA*
- *STUDENCI (RÓŻNE KIERUNKI)*

Ankieta na temat bezpieczeństwa systemu informacyjnego w organizacji publicznej na przykładzie uczelni wyższej, skierowana do *nauczycieli akademickich, kadry administracyjnej, studentów*

Ankieta służy poznaniu opinii użytkowników, nauczycieli akademickich, kadry administracyjnej i studentów w zakresie bezpieczeństwa systemu informacyjnego w uczelni wyższej. Ma ona charakter anonimowy a zebrane wyniki posłużą opracowaniu statystycznemu w celu określenia poziomu bezpieczeństwa systemu informacyjnego w uczelni wyższej.

Organizacja i zasady użytkowania systemu informacyjnego w uczelni wyższej:

1. W jaki sposób najczęściej Państwo przekazujecie i odbieracie informacje w uczelni wyższej?

(odpowiedź proszę zaznaczyć w skali 1-5, gdzie: 1 oznacza-najrzadziej wykorzystywany kanał informacji, zaś 5 oznacza-najczęściej wykorzystywany kanał informacji)

Lp.	**Kanały obiegu informacji**	**Skala 1-5**				
1	Wirtualna Uczelnia, Dziekanat10	1	2	3	4	5
2	Informacje na piśmie	1	2	3	4	5
3	Przekaz ustny	1	2	3	4	5
4	Poczta elektroniczna	1	2	3	4	5
5	Aplikacja MsTeams	1	2	3	4	5

Rozkład odpowiedzi respondentów w kwestionariuszu ankiety dla nauczycieli akademickich, kadry administracyjnej, studentów (różne kierunki):

Odpowiedzi respondentów – najczęstszy kanał przekazywania informacji				
Osoby poddane badaniu	**Respondenci, nauczyciele akademiccy, kadra administracyjna**	**Respondenci, nauczyciele akademiccy, studenci (różne kierunki)**	**Respondenci, kadra administracyjna, studenci (różne roczniki)**	**Ogólna ocena**
	Skala 1-5	***Skala 1-5***	***Skala 1-5***	***Skala 1-5***
Wirtualna uczelnia, uczelnia 10/USOS	**4,84**	**2,97**	**2,89**	**3,57**
Przekaz na piśmie	**3,09**	**3,56**	**4,20**	**3,62**
Przekaz ustny	**3,91**	**4,88**	**3,34**	**4,04**
Poczta elektroniczna	**3,74**	**3,64**	**4,10**	**3,83**
Aplikacja MsTeams	**2,39**	**3,15**	**2,67**	**2,74**

Poniżej odpowiedziom zostały nadane rangi, co do częstotliwości przekazywania i odbierania informacji w uczelni wyższej.

Ranga 1:

- Przekaz ustny

Ranga 2:

- Poczta elektroniczna

Ranga 3:

- Przekaz na piśmie

Ranga 4:

- Wirtualna uczelnia/Uczelnia 10/USOS

Ranga 5:

- Aplikacja MsTeams

2. Czy utrzymujecie Państwo w tajemnicy hasło, mające umożliwić dostęp do zasobów w sieci?

(w polu proszę wstawić znak „X”)

TAK	**NIE**

Rozkład odpowiedzi respondentów w kwestionariuszu ankiety dla nauczycieli akademickich, kadry administracyjnej, studentów (różne kierunki):

Odpowiedzi badanych osób Tajemnica hasła dostępu do zasobów w sieci							
Osoby poddane badaniu		**Respondenci nauczyciele akademiccy**		**Respondenci kadra administracyjna**		**Respondenci studenci (różne kierunki)**	
Ocena		*liczba wskazań*	*udział procentowy*	*liczba wskazań*	*udział procentowy*	*liczba wskazań*	*udział procentowy*
TAK	**KOBIETY**	295	59%	458	91,6%	356	71,2%
	MĘŻCZYŹNI	201	40,2%	42	8,4%	107	21,4%
NIE	**KOBIETY**	3	0,6%	0	0,0%	25	5%
	MĘŻCZYŹNI	1	0,2%	0	0,0%	12	2,4%
		500	**100%**	**500**	**100%**	**1000**	**500**

3. Czy stosujecie Państwo zasady bezpieczeństwa w posługiwaniu się loginem oraz hasłem do systemu?

(w polu proszę wstawić znak „X")

TAK	**NIE**

Rozkład odpowiedzi respondentów w kwestionariuszu ankiety dla nauczycieli akademickich, kadry administracyjnej, studentów (różne kierunki):

Odpowiedzi badanych osób Zachowanie bezpieczeństwa w posługiwaniu się loginem i hasłem do systemu							
Osoby poddane badaniu		**Respondenci nauczyciele akademiccy**		**Respondenci kadra administracyjna**		**Respondenci studenci (różne kierunki)**	
Ocena		*liczba wskazań*	*udział procentowy*	*liczba wskazań*	*udział procentowy*	*liczba wskazań*	*udział procentowy*
TAK	**KOBIETY**	295	59%	458	91,6%	354	70,8%
	MĘŻCZYŹNI	201	40,2%	42	8,4%	107	21,4%
NIE	**KOBIETY**	3	0,6%	0	0,0%	27	5,4%
	MĘŻCZYŹNI	1	0,2%	0	0,0%	12	2,4%
		500	**100%**	**500**	**100%**	**1000**	**500**

4. Czy w przypadku utraty hasła lub podejrzenia, że hasło zostało wykradzione i odczytane przez osobę do tego nieupoważnioną, informujecie Państwo o tym fakcie administratora systemu informacyjnego?

(w polu proszę wstawić znak „X")

TAK	**NIE**

Rozkład odpowiedzi respondentów w kwestionariuszu ankiety dla nauczycieli akademickich, kadry administracyjnej, studentów (różne kierunki):

Odpowiedzi badanych osób Informowanie administratora przez użytkowników uczelnianego systemu w przypadku utraty hasła lub podejrzenia, że zostało odczytane/wykorzystane przez osobę nieuprawnioną							
Osoby poddane badaniu		**Respondenci nauczyciele akademiccy**		**Respondenci kadra administracyjna**		**Respondenci studenci (różne kierunki)**	
Ocena		***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***
TAK	**KOBIETY**	237	47,4%	440	88%	251	50,2%
	MĘŻCZYŹNI	186	37,2%	35	7%	84	16,8%
NIE	**KOBIETY**	61	12,2%	18	3,6%	130	26%
	MĘŻCZYŹNI	16	3,2%	7	1,4%	35	7%
		500	**100%**	**500**	**100%**	**1000**	**500**

5. Czy dokonujecie Państwo po zalogowaniu sprawdzenia wiarygodności informacji odnośnie swojego ostatniego udanego logowania do systemu w uczelni wyższej?

(w polu proszę wstawić znak „X”)

TAK	**NIE**

Rozkład odpowiedzi respondentów w kwestionariuszu ankiety dla nauczycieli akademickich, kadry administracyjnej, studentów (różne kierunki):

Odpowiedzi badanych osób Sprawdzenie wiarygodności informacji odnośnie swojego ostatniego udanego logowania do systemu uczelni wyższej					
Osoby poddane badaniu	**Respondenci nauczyciele akademiccy**		**Respondenci kadra administracyjna**		**Respondenci studenci (różne kierunki)**	
Ocena	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***
TAK	263	52,6%	382	76,4%	48	9,6%
NIE	237	47,4%	118	23,6%	452	90,4%
	500	**100%**	**500**	**100%**	**500**	**100%**

6. Czy w przypadku stwierdzenia przez Państwa nieścisłości na koncie w systemie, osobiście o tym fakcie informujecie Państwo administratora uczelnianego odpowiedzialnego za system informacyjny?

(w polu proszę wstawić znak „X")

TAK **NIE**

Rozkład odpowiedzi respondentów w kwestionariuszu ankiety dla nauczycieli akademickich, kadra administracyjna, studenci (różne kierunki):

Odpowiedzi badanych osób Osobiste informowanie uczelnianego administratora odpowiedzialnego za system informacyjny?						
Osoby poddane badaniu	**Respondenci nauczyciele akademiccy**		**Respondenci kadra administracyjna**		**Respondenci Studenci (różne kierunki)**	
Ocena	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***
TAK	490	98%	500	100%	440	88%
NIE	10	2%	0	0%	60	12%
	500	**100%**	**500**	**100%**	**500**	**100%**

7. Czy w przypadku korzystania z prywatnego komputera lub laptopa w dostępie do systemów wewnętrznych zachowują Państwo wszystkie zasady ochrony danych osobowych stosowane w uczelni wyższej?

(w polu proszę wstawić znak „X")

TAK **NIE**

Rozkład odpowiedzi respondentów w kwestionariuszu ankiety dla nauczycieli akademickich, kadra administracyjna, studenci (różne kierunki):

Odpowiedzi badanych osób Zachowanie wszystkich zasad ochrony danych osobowych stosowanych w uczelni wyższej przez użytkowników w przypadku korzystania z prywatnego komputera lub laptopa w dostępie do systemów wewnętrznych						
Osoby poddane badaniu	**Respondenci nauczyciele akademiccy**		**Respondenci kadra administracyjna**		**Respondenci studenci (różne kierunki)**	
Ocena	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***

TAK	500	100%	500	100%	465	93%
NIE	0	0%	0	0%	35	7%
	500	**100%**	**500**	**100%**	**500**	**100%**

8. Czy korzystając z prywatnego komputera/laptopa, w dostępie do systemu informacyjnego zdarza się Państwu ujawnić dane innym osobom do tego nieupoważnionym?

(w polu proszę wstawić znak „X")

TAK	**NIE**

Rozkład odpowiedzi respondentów w kwestionariuszu ankiety dla nauczycieli akademickich, kadra administracyjna, studenci (różne kierunki):

Odpowiedzi badanych osób **Ujawnienie danych osobom nieupoważnionym w przypadku korzystania z prywatnego komputera/laptopa w dostępie do systemów wewnętrznych uczelni**						
Osoby poddane badaniu	**Respondenci nauczyciele akademiccy**		**Respondenci kadra administracyjna**		**Respondenci studenci (różne kierunki)**	
Ocena	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***
TAK	0	0%	0	0%	188	37,6%
NIE	500	100%	500	100%	312	62,4%
	500	**100%**	**500**	**100%**	**500**	**100%**

9. Czy korzystacie Państwo podczas logowania z dostępnymi instrukcjami ułatwiającymi korzystanie z systemu informacyjnego?

(w polu proszę wstawić znak „X")

TAK	**NIE**

Rozkład odpowiedzi respondentów w kwestionariuszu ankiety dla nauczycieli akademickich, kadra administracyjna, studenci (różne kierunki):

Odpowiedzi badanych osób *zapoznania się przez nich z dostępnymi instrukcjami ułatwiającymi korzystanie z systemu informacyjnego w uczelni wyższej*						
Osoby poddane badaniu	**Respondenci nauczyciele akademiccy**		**Respondenci kadra administracyjna**		**Respondenci studenci (różne kierunki)**	
Ocena	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***
TAK	492	98,4%	500	100%	267	53,4%
NIE	8	1,6%	0	0%	233	46,6%
	500	**100%**	**500**	**100%**	**500**	**100%**

10. Czy korzystacie Państwo z konta indywidualnego, systemu informatycznego założonego każdemu pracownikowi uczelni/studentowi uczelni?

(w polu proszę wstawić znak „X")

Lp.	***Korzystanie z konta indywidualnego systemu informacyjnego***	***W polu proszę zaznaczyć prawidłową odpowiedź***
1	***TAK*** ☐	☐ częściej niż raz dziennie ☐ raz dziennie ☐ 2-3 razy w tygodniu ☐ raz w tygodniu ☐ rzadziej niż raz w tygodniu
2	***NIE*** ☐	

Rozkład odpowiedzi respondentów w kwestionariuszu ankiety dla nauczycieli akademickich, kadry administracyjnej, studentów (różne kierunki):

Odpowiedzi badanych osób ***Korzystanie z konta indywidualnego, systemu informatycznego założonego każdemu pracownikowi w uczelni wyższej***						
Odpowiedź	**Respondenci nauczyciele akademiccy**		**Respondenci kadra administracyjna**		**Respondenci studenci (różne kierunki)**	
TAK	*liczba wskazań*	*udział procentowy*	*liczba wskazań*	*udział procentowy*	*liczba wskazań*	*udział procentowy*
częściej niż raz dzienni	467	93,4%	487	97,4%	4	0,8%
raz dziennie	28	5,6%	13	2,6%	28	5,6%
2-3 razy w tygodniu	5	1%	0	0%	128	25,6%
raz w tygodniu	0	0%	0	0%	186	37,2%
rzadziej niż raz w tygodniu	0	0%	0	0%	154	30,8%
NIE	0	0%	0	0%	0	0%
	500	**100%**	**500**	**100%**	**500**	**100%**

Rozkład odpowiedzi respondentów w kwestionariuszu ankiety dla nauczycieli akademickich, kadra administracyjna, studenci (różne kierunki):

11. Czy korzystając z konta indywidualnego jak i ogólnego systemu informatycznego w uczelni wyższej zdarza się Państwu:

(w polu proszę wstawić znak „X")

Lp.	***Przykładowe przyczyny wycieku danych poprzez:***	
1	**Zapomnienie hasła**	☐ **TAK** **bardzo często** ☐ **często** ☐ **rzadko** ☐ **bardzo rzadko** ☐ **sporadycznie** ☐ ☐ **NIE**

<table>
<tr><td>2</td><td>Udostępnienie skorzystania ze swojego konta osobom nieupoważnionym</td><td>☐ TAK<table><tr><td>bardzo często</td><td></td></tr><tr><td>często</td><td></td></tr><tr><td>rzadko</td><td></td></tr><tr><td>bardzo rzadko</td><td></td></tr><tr><td>sporadycznie</td><td></td></tr></table>☐ NIE</td></tr>
<tr><td>3</td><td>Ujawnienie hasła osobom do tego nieupoważnionym</td><td>☐ TAK<table><tr><td>bardzo często</td><td></td></tr><tr><td>często</td><td></td></tr><tr><td>rzadko</td><td></td></tr><tr><td>bardzo rzadko</td><td></td></tr><tr><td>sporadycznie</td><td></td></tr></table>☐ NIE</td></tr>
<tr><td>4</td><td>Nie wylogowanie się z konta</td><td>☐ TAK<table><tr><td>bardzo często</td><td></td></tr><tr><td>często</td><td></td></tr><tr><td>rzadko</td><td></td></tr><tr><td>bardzo rzadko</td><td></td></tr><tr><td>sporadycznie</td><td></td></tr></table>☐ NIE</td></tr>
</table>

- ***Zapomnienie hasła***

Odpowiedzi badanych osób Zapomnienie hasła						
Odpowiedź	**Respondenci nauczyciele akademiccy**		**Respondenci kadra administracyjna**		**Respondenci studenci (różne kierunki)**	
TAK	*liczba wskazań*	*udział procentowy*	*liczba wskazań*	*udział procentowy*	*liczba wskazań*	*udział procentowy*
bardzo często	0	0%	0	0%	0	0%
często	0	0%	0	0%	0	0%
rzadko	5	1%	0	0%	6	1,2%
bardzo rzadko	69	13,8%	2	0,4%	15	3%
sporadycznie	398	79,6%	40	8%	196	39,2%
NIE	28	5,6%	458	91,6%	283	56,6%
	500	**100%**	**500**	**100%**	**500**	**100%**

- ***Udostępnienie skorzystania ze swojego konta osobom nieupoważnionym***

Odpowiedzi badanych osób Udostępnienie skorzystania ze swojego konta osobom nieupoważnionym						
Odpowiedź	**Respondenci nauczyciele akademiccy**		**Respondenci kadra administracyjna**		**Respondenci studenci (różne kierunki)**	
TAK	*liczba wskazań*	*udział procentowy*	*liczba wskazań*	*udział procentowy*	*liczba wskazań*	*udział procentowy*
bardzo często	0	0%	0	0%	0	0%
często	0	0%	0	0%	0	0%
rzadko	0	0%	0	0%	2	0,4%
bardzo rzadko	6	1,2%	0	0%	32	6,4%
sporadycznie	38	7,6%	11	2,2%	156	31,2%
NIE	456	91,2%	489	97,8%	310	62%
	500	**100%**	**500**	**100%**	**500**	**100%**

- ***Ujawnienie hasła osobom do tego nieupoważnionym***

Odpowiedzi badanych osób Ujawnienie hasła osobom do tego nieupoważnionym						
Odpowiedź	**Respondenci nauczyciele akademiccy**		**Respondenci kadra administracyjna**		**Respondenci studenci (różne kierunki)**	
TAK	*liczba wskazań*	*udział procentowy*	*liczba wskazań*	*udział procentowy*	*liczba wskazań*	*udział procentowy*

bardzo często	0	0%	0	0%	0	0%
często	0	0%	0	0%	0	0%
rzadko	0	0%	0	0%	0	0%
bardzo rzadko	0	0%	0	0%	0	0%
sporadycznie	2	0,4%	0	0%	102	20,4%
NIE	498	99,6%	500	100%	398	79,6%
	500	**100%**	**500**	**100%**	**500**	**100%**

- ***Nie wylogowanie się z konta***

Odpowiedzi badanych osób Nie wylogowanie się z konta						
Odpowiedź	**Respondenci nauczyciele akademiccy**		**Respondenci kadra administracyjna**		**Respondenci studenci (różne kierunki)**	
TAK	*liczba wskazań*	*udział procentowy*	*liczba wskazań*	*udział procentowy*	*liczba wskazań*	*udział procentowy*
bardzo często	0	0%	0	0%	0	0%
często	0	0%	0	0%	12	2,4%
rzadko	49	0,2%	0	0%	46	9,2%
bardzo rzadko	89	17,8%	0	0%	128	25,6%
sporadycznie	159	31,8%	5	1%	125	25%
NIE	203	40,6%	495	99%	189	37,8%
	500	**100%**	**500**	**100%**	**500**	**100%**

12. Czy Państwa informacje, dane, wydruki, eksporty, korespondencja itd. są bezpieczne w systemie informacyjnym w uczelni wyższej?

(w polu proszę wstawić znak „X")

TAK	**NIE**

Odpowiedzi badanych osób *Bezpieczeństwo danych w systemie informacyjnym w uczelni wyższej*						
Osoby poddane badaniu	**Respondenci nauczyciele akademiccy**		**Respondenci kadra administracyjna**		**Respondenci studenci (różne kierunki)**	
Ocena	*liczba wskazań*	*udział procentowy*	*liczba wskazań*	*udział procentowy*	*liczba wskazań*	*udział procentowy*
TAK	446	89,2%	478	95,6%	404	80,8%
NIE	54	10,8%	22	4,4%	96	19,2%
	500	**100%**	**500**	**100%**	**500**	**100%**

13. Jak Państwo oceniają zagrożenia systemu informacyjnego w uczelni wyższej

(w polu proszę wstawić znak „X")

Lp.	*Występujące zagrożenia*	*Ocena respondentów*				
		bardzo niska	*niska*	*przeciętna*	*wysoka*	*bardzo wysoka*
1	*Klęski żywiołowe, pożar*					
2	*Utrata danych*					
3	*Zmiana hasła przez osoby trzecie i brak dostępu do własnego konta użytkownika*					
4	*Rozkodowanie hasła dostępu*					
5	*Cyberatak*					
6	*Przekazywanie informacji osobom nieuprawnionym*					
7	*Celowe pozorowanie awarii systemu*					
8	*Wykorzystywanie luk w zabezpieczeniach dostępu do poczty elektronicznej i serwisu informacyjnego*					
9	*Programy wykorzystujące błędy w systemach operacyjnych i oprogramowaniu użytkowym*					
10	*Wirusy, robaki, konie trojańskie*					
11	*Obecność podejrzanego oprogramowania*					

12	***Manipulacja danymi w systemie***					
13	***Ujawnienie informacji podczas przesyłania***					
14	***Podszywanie się pod inną osobę***					
15	***Błędy, wady oprogramowania***					
16	***Awarie sprzętowe i oprogramowania***					
17	***Pozostawienie danych wrażliwych na biurkach, półkach w miejscach do tego nieprzeznaczonych***					

- ***Klęski żywiołowe, pożar***

Odpowiedzi badanych osób: klęski żywiołowe, pożar						
Osoby poddane badaniu	**Respondenci nauczyciele akademiccy**		**Respondenci kadra administracyjna**		**Respondenci studenci (różne kierunki)**	
Ocena	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***
bardzo niska	345	69%	328	65,6%	192	38,4%
niska	85	17%	89	17,8%	125	25%
przeciętna	35	7%	36	7,2%	150	30%
wysoka	28	5,6%	21	4,2%	19	3,8%
bardzo wysoka	7	1,4%	26	5,2%	14	2,8%
	500	**100%**	**500**	**100%**	**500**	**100%**

- ***Utrata danych***

Odpowiedzi badanych osób utrata danych						
Osoby poddane badaniu	**Respondenci nauczyciele akademiccy**		**Respondenci kadra administracyjna**		**Respondenci studenci (różne kierunki)**	
Ocena	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***
bardzo niska	35	7%	17	3,4%	92	18,4%
niska	26	5,2%	18	3,6%	165	33%
przeciętna	378	75,6%	96	19,2%	178	35,6%
wysoka	33	6,6%	82	16,4%	36	7,2%
bardzo wysoka	28	5,6%	287	57,4%	29	5,8%
	500	**100%**	**500**	**100%**	**500**	**100%**

- ***Zmiana hasła przez osoby trzecie i brak dostępu do własnego konta użytkownika***

Odpowiedzi badanych osób zmiana hasła przez osoby trzecie i brak dostępu do własnego konta użytkownika						
Osoby poddane badaniu	**Respondenci nauczyciele akademiccy**		**Respondenci kadra administracyjna**		**Respondenci Studenci (różne kierunki)**	
Ocena	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***
bardzo niska	15	3%	31	6,2%	17	3,4%
niska	159	31,8%	129	25,8%	83	16,6%
przeciętna	281	56,2%	312	62,4%	362	72,4%
wysoka	25	5%	12	2,4%	34	6,8%
bardzo wysoka	20	4%	16	3,2%	4	0,8%
	500	**100%**	**500**	**100%**	**500**	**100%**

- ***Rozkodowanie hasła dostępu***

Odpowiedzi badanych osób rozkodowanie hasła dostępu						
Osoby poddane badaniu	**Respondenci nauczyciele akademiccy**		**Respondenci kadra administracyjna**		**Respondenci studenci (różne kierunki)**	
Ocena	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***
bardzo niska	265	53%	289	57,8%	238	47,6%
niska	169	33,8%	195	39%	85	17%
przeciętna	25	5%	9	1,8%	99	19,8%
wysoka	26	5,2%	4	0,8%	37	7,4%
bardzo wysoka	16	3,2%	5	1%	41	8,2%
	500	**100%**	**500**	**100%**	**500**	**100%**

- ***Cyberatak***

Odpowiedzi badanych osób cyberatak						
Osoby poddane badaniu	**Respondenci nauczyciele akademiccy**		**Respondenci kadra administracyjna**		**Respondenci studenci (różne kierunki)**	
Ocena	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***
bardzo niska	412	82,4%	389	77,8%	289	57,8%
niska	35	7%	42	8,4%	115	23%
przeciętna	18	3,6%	26	5,2%	45	9%
wysoka	19	3,8%	24	4,8%	26	5,2%
bardzo wysoka	16	3,2%	19	3,8%	25	5%
	500	**100%**	**500**	**100%**	**500**	**100%**

- ***Przekazywanie informacji osobom nieuprawnionym***

Odpowiedzi badanych osób przekazywanie informacji osobom nieuprawnionym						
Osoby poddane badaniu	**Respondenci nauczyciele akademiccy**		**Respondenci kadra administracyjna**		**Respondenci Studenci (różne kierunki)**	
Ocena	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***
bardzo niska	429	85,8%	435	87%	298	59,6%
niska	36	7,2%	28	5,6%	168	33,6%
przeciętna	18	3,6%	17	3,4%	12	2,4%
wysoka	15	3%	15	3%	13	2,6%
bardzo wysoka	2	0,4%	5	1%	9	1,8%
	500	**100%**	**500**	**100%**	**500**	**100%**

- ***Celowe pozorowanie awarii systemu***

Odpowiedzi badanych osób celowe pozorowanie awarii systemu						
Osoby poddane badaniu	**Respondenci nauczyciele akademiccy**		**Respondenci kadra administracyjna**		**Respondenci studenci (różne kierunki)**	
Ocena	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***
bardzo niska	437	87,4%	443	88,6%	276	55,2%
niska	38	7,6%	19	3,8%	189	37,8%
przeciętna	15	3%	15	3%	16	3,2%
wysoka	8	1,6%	16	3,2%	15	3%
bardzo wysoka	2	0,4%	7	1,4%	9	1,8%
	500	**100%**	**500**	**100%**	**500**	**100%**

- ***Wykorzystywanie luk w zabezpieczeniach dostępu do poczty elektronicznej i serwisu informacyjnego***

Odpowiedzi badanych osób wykorzystywanie luk w zabezpieczeniach dostępu do poczty elektronicznej i serwisu informacyjnego						
Osoby poddane badaniu	**Respondenci nauczyciele akademiccy**		**Respondenci kadra administracyjna**		**Respondenci studenci (różne kierunki)**	
Ocena	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***
bardzo niska	16	3,2%	259	51,8%	162	32,4%
niska	423	84,6%	169	33,8%	255	51%
przeciętna	28	5,6%	46	9,2%	45	9%
wysoka	19	3,8%	23	4,6%	29	5,8%
bardzo wysoka	14	2,8%	3	3%	9	1,8%
	500	**100%**	**500**	**100%**	**500**	**100%**

Programy wykorzystujące błędy w systemach operacyjnych i oprogramowaniu użytkowym

Odpowiedzi badanych osób programy wykorzystujące błędy w systemach operacyjnych i w oprogramowaniu użytkowym						
Osoby poddane badaniu	**Respondenci nauczyciele akademiccy**		**Respondenci kadra administracyjna**		**Respondenci studenci (różne kierunki)**	
Ocena	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***
bardzo niska	42	8,4%	198	39,6%	62	12,4%
niska	248	49,6%	262	52,4%	238	47,6%
przeciętna	179	35,8%	23	4,6%	168	33,6%
wysoka	22	4,4%	7	1,4%	26	5,2%
bardzo wysoka	9	1,8%	10	2%	6	1,2%
	500	**100%**	**500**	**100%**	**500**	**100%**

- ***Wirusy, robaki, konie trojańskie***

Odpowiedzi badanych osób wirusy, robaki, konie trojańskie						
Osoby poddane badaniu	**Respondenci nauczyciele akademiccy**		**Respondenci kadra administracyjna**		**Respondenci studenci (różne kierunki)**	
Ocena	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***
bardzo niska	162	32,4%	59	11,8%	45	9%
niska	243	48,6%	265	53%	289	57,8%
przeciętna	39	7,8%	129	25,8%	123	24,6%
wysoka	27	5,4%	38	7,6%	32	6,4%
bardzo wysoka	29	5,8%	9	1,8%	11	2,2%
	500	**100%**	**500**	**100%**	**500**	**100%**

- ***Obecność podejrzanego oprogramowania***

Odpowiedzi badanych osób obecność podejrzanego oprogramowania						
Osoby poddane badaniu	**Respondenci nauczyciele akademiccy**		**Respondenci kadra administracyjna**		**Respondenci studenci (różne kierunki)**	
Ocena	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***
bardzo niska	244	48,8%	298	59,6%	169	33,8%
niska	189	37,8%	168	33,6%	312	62,4%
przeciętna	39	7,8%	28	5,6%	17	3,4%
wysoka	17	3,4%	4	0,8%	2	0,4%
bardzo wysoka	11	2,2%	2	0,4%	0	0,0%
	500	**100%**	**500**	**100%**	**500**	**100%**

- ***Manipulacja danymi w systemie***

Odpowiedzi badanych osób manipulacja danymi w systemie						
Osoby poddane badaniu	**Respondenci nauczyciele akademiccy**		**Respondenci kadra administracyjna**		**Respondenci studenci (różne kierunki)**	
Ocena	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***
bardzo niska	69	13,8%	142	28,4%	59	11,8%
niska	346	69,2%	296	59,2%	268	53,6%
przeciętna	39	7,8%	29	5,8%	159	31,8%
wysoka	29	5,8%	28	5,6%	8	1,6%
bardzo wysoka	17	3,4%	5	1%	6	1,2%
	500	**100%**	**500**	**100%**	**500**	**100%**

- ***Ujawnienie informacji podczas przesyłania***

Odpowiedzi badanych osób ujawnienie informacji podczas przesyłania						
Osoby poddane badaniu	**Respondenci nauczyciele akademiccy**		**Respondenci kadra administracyjna**		**Respondenci studenci (różne kierunki)**	
Ocena	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***
bardzo niska	278	55,6%	119	23,8%	169	33,8%
niska	168	33,6%	238	47,6%	289	57,8%
przeciętna	26	5,2%	98	19,6%	35	7%
wysoka	18	3,6%	39	7,8%	5	1%
bardzo wysoka	10	2%	6	1,2%	2	0,4%
	500	**100%**	**500**	**100%**	**500**	**100%**

- ***Podszywanie się pod inną osobę***

Odpowiedzi badanych osób podszywanie się pod inną osobę						
Osoby poddane badaniu	**Respondenci nauczyciele akademiccy**		**Respondenci kadra administracyjna**		**Respondenci studenci (różne kierunki)**	
Ocena	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***
bardzo niska	312	62,4%	89	17,8%	193	38,6%
niska	89	17,8%	342	68,4%	278	55,6%
przeciętna	85	17%	49	9,8%	18	3,6%
wysoka	6	1,2%	17	34%	6	1,2%
bardzo wysoka	8	1,6%	3	0,6%	5	1%
	500	**100%**	**500**	**100%**	**500**	**100%**

- ***Błędy, wady oprogramowania***

• **Odpowiedzi badanych osób błędy, wady oprogramowania**						
Osoby poddane badaniu	**Respondenci nauczyciele akademiccy**		**Respondenci kadra administracyjna**		**Respondenci studenci (różne kierunki)**	
Ocena	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***
bardzo niska	89	17,8%	46	9,2%	198	39,6%

niska	99	19,8%	389	77,8%	158	31,6%
przeciętna	259	51,8%	28	5,6%	129	25,8%
wysoka	49	9,8%	30	6%	12	2,4%
bardzo wysoka	4	0,8%	7	1,4%	3	0,6%
	500	**100%**	**500**	**100%**	**500**	**100%**

- ***Awarie sprzętowe i oprogramowania***

Odpowiedzi badanych osób awarie sprzętowe i oprogramowania						
Osoby poddane badaniu	**Respondenci nauczyciele akademiccy**		**Respondenci kadra administracyjna**		**Respondenci studenci (różne kierunki)**	
Ocena	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***
bardzo niska	189	37,8%	139	27,8%	59	11,8%
niska	172	34,4%	169	33,8%	112	22,4%
przeciętna	122	24,4%	182	36,4%	298	59,6%
wysoka	15	3%	9	1,8%	25	5%
bardzo wysoka	2	0,4%	1	0,2%	6	1,2%
	500	**100%**	**500**	**100%**	**500**	**100%**

- ***Pozostawienie danych wrażliwych na biurkach, półkach w miejscach do tego nieprzeznaczonych***

Odpowiedzi badanych osób pozostawienie danych wrażliwych na biurkach, półkach w miejscach do tego nieprzeznaczonych						
Osoby poddane badaniu	**Respondenci nauczyciele akademiccy**		**Respondenci kadra administracyjna**		**Respondenci studenci (różne kierunki)**	
Ocena	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***
bardzo niska	69	13,8%	63	12,6%	169	33,8%
niska	116	23,2%	146	29,2%	158	31,6%
przeciętna	269	53,8%	246	49,2%	162	32,4%
wysoka	28	5,6%	29	5,8%	8	1,6%
bardzo wysoka	19	3,8%	16	3,2%	3	0,6%
	500	**100%**	**500**	**100%**	**500**	**100%**

14. Kto według Państwa jest najczęstszym odbiorcą Państwa informacji w systemie?

(w polu proszę wstawić znak „X")

Lp.	***Odbiorcy informacji w systemie***	***Odpowiedzi respondentów***
1	**Rektor/Prorektorzy/Władze Uczelni**	
2	**Dyrektorzy Instytutów**	
3	**Centrum Obslugi studenta**	
4	**Kancelaria uczelni**	
5	**Sekretariat (jednostki administracyjne)**	

Rozkład odpowiedzi respondentów w kwestionariuszu ankiety dla nauczycieli akademickich, kadry administracyjnej, studentów (różne kierunki):

Odpowiedzi badanych osób odbiór informacji w systemie						
Osoby poddane badaniu	**Respondenci nauczyciele akademiccy**		**Respondenci kadra administracyjna**		**Respondenci studenci (różne kierunki)**	
Ocena	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***
Rektor/Prorektorzy/Władze Uczelni	15	3%	32	6,4%	2	0,4%
Dyrektorzy Instytutów	25	5%	49	9,8%	6	1,2%
Centrum Obsługi studenta	6	1,2%	65	13%	172	34,4%
Kancelaria uczelni	158	31,6%	158	31,6%	152	30,4%
Sekretariat (jednostki administracyjne)	296	59,2%	196	39,2%	168	33,6%
	500	**100%**	**500**	**100%**	**500**	**100%**

15. Czy Państwa zdaniem uzyskanie większego poziomu bezpieczeństwa systemu informacyjnego w uczelni wyższej jest możliwe przez:

(w polu proszę wstawić znak „X")

Lp.	*Większy poziom bezpieczeństwa*	*Odpowiedzi respondentów*	
		TAK	**NIE**
1	***Ograniczenie dostępu do danych nieupoważnionym osobom***		
2	***Zwiększenie świadomości o zagrożeniach jakie mogą wystąpić w konsekwencji błędnego korzystania z systemu informacyjnego wśród użytkowników***		
3	***Reagowanie na incydenty mające związek z naruszeniem bezpieczeństwa systemu informacyjnego***		
4	***Zwiększenie kontroli użytkowników systemu informacyjnego***		
5	***Wykorzystanie nowoczesnego sprzętu komputerowego***		

6	***Stosowanie dobrze zabezpieczonych zewnętrznych nośników danych***	**TAK** **NIE**
7	***Zgłaszanie wszelkich zauważonych błędów i niedoskonałości systemowych***	**TAK** **NIE**

W tym pytaniu tak samo jak w pierwszym zostały wyłonione:

Rangi nauczyciele akademiccy i kadra administracyjna

Ranga 1:

- ograniczenie osobom nieupoważnionym dostępu do danych;
- reagowanie na incydenty, związane z naruszeniem bezpieczeństwa systemu informacyjnego;
- wykorzystanie nowoczesnego sprzętu komputerowego;

Ranga 2:

- zwiększenie świadomości wśród użytkowników o zagrożeniach, jakie mogą wystąpić w konsekwencji niewłaściwego korzystania z systemu informacyjnego;

Ranga 3:

- zgłaszanie wszelkich zauważonych błędów i niedoskonałości systemowych;

Ranga 4:

- stosowanie dobrze zabezpieczonych zewnętrznych nośników danych

Ranga 5:

zwiększenie kontroli użytkowników systemu informacyjnego.

Rangi nauczyciele akademiccy i studenci (różne kierunki)

Ranga 1:

- wykorzystanie nowoczesnego sprzętu komputerowego;

Ranga 2:

- reagowanie na incydenty, związane z naruszeniem bezpieczeństwa systemu informacyjnego;

Ranga 3:

- zgłaszanie wszelkich zauważonych błędów i niedoskonałości systemowych;

Ranga 4:

- stosowanie dobrze zabezpieczonych zewnętrznych nośników danych

Ranga 5:

- ograniczenie osobom nieupoważnionym dostępu do danych;

Ranga 6:

- zwiększenie świadomości wśród użytkowników o zagrożeniach jakie mogą wystąpić w konsekwencji niewłaściwego korzystania z systemu informacyjnego;

Ranga 7:

- zwiększenie kontroli użytkowników systemu informacyjnego

Rangi kadra administracyjna i studenci (różne kierunki)

Ranga 1:

- wykorzystanie nowoczesnego sprzętu komputerowego;

Ranga 2:

- zgłaszanie wszelkich zauważonych błędów i niedoskonałości systemowych;

Ranga 3:

- reagowanie na incydenty, związane z naruszeniem bezpieczeństwa systemu informacyjnego;

Ranga 4:

- stosowanie dobrze zabezpieczonych zewnętrznych nośników danych;

Ranga 5:

- ograniczenie osobom nieupoważnionym dostępu do danych;

Ranga 6:

- zwiększenie świadomości wśród użytkowników o zagrożeniach jakie mogą wystąpić w konsekwencji niewłaściwego korzystania z systemu informacyjnego;

Ranga 7:

zwiększenie kontroli użytkowników systemu informacyjnego

Rozkład odpowiedzi respondentów w kwestionariuszu ankiety dla nauczycieli akademickich, kadry administracyjnej, studentów (różne kierunki):

ograniczenie osobom nieupoważnionym dostępu do danych						
Osoby poddane badaniu	**Respondenci nauczyciele akademiccy**		**Respondenci kadra administracyjna**		**Respondenci studenci (różne kierunki)**	
ODPOWIEDŹ	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***
TAK	500	100%	500	100%	328	65,6%
NIE	0	0%	0	0%	172	34,4%
	500	100%	500	100%	500	100%
zwiększenie świadomości wśród użytkowników o zagrożeniach jakie mogą wystąpić w konsekwencji niewłaściwego korzystania z systemu informacyjnego						
Osoby poddane badaniu	**Respondenci nauczyciele akademiccy**		**Respondenci kadra administracyjna**		**Respondenci studenci (różne kierunki)**	
ODPOWIEDŹ	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***
TAK	480	96%	500	100%	285	57%
NIE	10	2%	0	0%	215	43%
	500	100%	500	100%	500	100%
zwiększenie kontroli użytkowników systemu informacyjnego						
Osoby poddane badaniu	**Respondenci nauczyciele akademiccy**		**Respondenci kadra administracyjna**		**Respondenci studenci (różne kierunki)**	
ODPOWIEDŹ	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***
TAK	478	95,6%	489	97,8%	279	55,8%
NIE	22	4,4%	11	2,2%	221	44,2%
	500	100%	500	100%	500	100%
reagowanie na incydenty, związane z naruszeniem bezpieczeństwa systemu informacyjnego						
Osoby poddane badaniu	**Respondenci nauczyciele akademiccy**		**Respondenci kadra administracyjna**		**Respondenci studenci (różne kierunki)**	
ODPOWIEDŹ	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***
TAK	500	100%	500	100%	381	76,2%
NIE	0	0%	0	0%	119	23,8%
	500	100%	500	100%	500	100%
zgłaszanie wszelkich zauważonych błędów i niedoskonałości systemowych						
Osoby poddane badaniu	**Respondenci nauczyciele akademiccy**		**Respondenci kadra administracyjna**		**Respondenci studenci (różne kierunki)**	
ODPOWIEDŹ	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***
TAK	478	95,6%	500	100%	392	78,4%
NIE	22	4,4%	0	0	108	21,6%
	500	100%	500	100%	500	100%
wykorzystanie nowoczesnego sprzętu komputerowego						
Osoby poddane badaniu	**Respondenci nauczyciele akademiccy**		**Respondenci kadra administracyjna**		**Respondenci studenci (różne kierunki)**	
ODPOWIEDŹ	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***
TAK	500	100%	500	100%	426	85,2%
NIE	0	0%	0	0%	74	14,8%
	500	100%	500	100%	500	100%
stosowanie dobrze zabezpieczonych zewnętrznych nośników danych						
Osoby poddane badaniu	**Respondenci nauczyciele akademiccy**		**Respondenci kadra administracyjna**		**Respondenci studenci (różne kierunki)**	
ODPOWIEDŹ	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***
TAK	479	95,8%	496	99,2%	356	71,2%

NIE	21	4,2%	4	0,8%	144	28,8%
	500	100%	500	100%	500	100%

16. Co Państwa zdaniem jest najczęstszym problemem w sprawach działania systemu w uczelni wyższej?

(w polu proszę wstawić znak „X")

Lp.	*Aspekt problemu*	*Ocena respondentów*				
		sporadycznie	*niska*	*przeciętna*	*wysoka*	*bardzo wysoka*
1	*Brak dostępu do Internetu*					
2	*Modernizacja systemu przez moderatora*					
3	*Awaria systemów*					
4	*Przestarzałe oprogramowania*					
5	*Niewystarczająca ilość komputerów*					

Rozkład odpowiedzi respondentów w kwestionariuszu ankiety dla nauczycieli akademickich, kadry administracyjnej, studentów (różne kierunki):

- ***Brak dostępu do Internetu***

Odpowiedzi badanych osób brak dostępu do internetu						
Osoby poddane badaniu	**Respondenci nauczyciele akademiccy**		**Respondenci kadra administracyjna**		**Respondenci studenci (różne kierunki)**	
Ocena	*liczba wskazań*	*udział procentowy*	*liczba wskazań*	*udział procentowy*	*liczba wskazań*	*udział procentowy*
sporadycznie	103	20,6%	76	15,2%	89	17,8%
niska	156	31,2%	102	20,4%	112	22,4%
przeciętna	118	23,6%	269	53,8%	236	47,2%
wysoka	89	17,8%	36	7,2%	34	6,8%
bardzo wysoka	34	6,8%	17	3,4%	29	5,8%
	500	**100%**	**500**	**100%**	**500**	**100%**

- ***Modernizacja systemu przez moderatora***

Odpowiedzi badanych osób modernizacja systemu przez moderatora						
Osoby poddane badaniu	**Respondenci nauczyciele akademiccy**		**Respondenci kadra administracyjna**		**Respondenci Studenci (różne kierunki)**	
Ocena	*liczba wskazań*	*udział procentowy*	*liczba wskazań*	*udział procentowy*	*liczba wskazań*	*udział procentowy*

sporadycznie	78	15,6%	89	17,8%	136	27,2%
niska	312	62,4%	189	37,8%	164	32,8%
przeciętna	68	13,6%	196	39,2%	158	31,6%
wysoka	28	5,6%	21	4,2%	31	6,2%
bardzo wysoka	14	2,8%	5	1%	11	2,2%
	500	**100%**	**500**	**100%**	**500**	**100%**

- ***Awaria systemów***

Odpowiedzi badanych osób awaria systemów						
Osoby poddane badaniu	**Respondenci nauczyciele akademiccy**		**Respondenci kadra administracyjna**		**Respondenci studenci (różne kierunki)**	
Ocena	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***
sporadycznie	80	16%	89	17,8%	89	17,8%
niska	114	22,8%	105	21%	159	31,8%
przeciętna	228	45,6%	268	53,6%	198	39,6%
wysoka	69	13,8%	31	6,2%	42	8,4%
bardzo wysoka	9	1,8%	7	1,4%	12	2,4%
	500	**100%**	**500**	**100%**	**500**	**100%**

- ***Przestarzałe oprogramowania***

Odpowiedzi badanych osób przestarzałe oprogramowania						
Osoby poddane badaniu	**Respondenci nauczyciele akademiccy**		**Respondenci kadra administracyjna**		**Respondenci studenci (różne kierunki)**	
Ocena	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***
sporadycznie	12	2,4%	21	4,2%	69	13,8%
niska	42	8,4%	86	17,2%	196	39,2%
przeciętna	412	82,4%	358	71,6%	189	37,8%
wysoka	30	6%	29	5,8%	29	5,8%
bardzo wysoka	4	0,8%	6	1,2%	17	3,4%
	500	**100%**	**500**	**100%**	**500**	**100%**

- ***Niewystarczająca ilość komputerów***

Odpowiedzi badanych osób niewystarczająca ilość komputerów						
Osoby poddane badaniu	**Respondenci nauczyciele akademiccy**		**Respondenci kadra administracyjna**		**Respondenci studenci (różne kierunki)**	
Ocena	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***
sporadycznie	68	13,6%	32	6,4%	79	15,8%

niska	119	23,8%	369	73,8%	116	23,2%
przeciętna	269	53,8%	89	17,8%	258	51,6%
wysoka	34	6,8%	5	1%	44	8,8%
bardzo wysoka	10	2%	5	1%	3	0,6%
	500	**100%**	**500**	**100%**	**500**	**100%**

17. Jaka jest Państwa ogólna ocena bezpieczeństwa systemu informacyjnego w uczelni wyższej?

(w polu proszę wstawić znak „X")

Lp.	*Jaka jest Państwa ogólna ocena bezpieczeństwa systemu informacyjnego w uczelni wyższej?*	*Odpowiedzi respondentów*
1	***bardzo niska***	
2	***niska***	
3	***przeciętna***	
4	***wysoka***	
5	***bardzo wysoka***	

Rozkład odpowiedzi respondentów w kwestionariuszu ankiety dla nauczycieli akademickich, kadry administracyjnej, studentów (różne kierunki):

Odpowiedzi badanych osób *stopień bezpieczeństwa systemu informacyjnego w uczelni wyższej*						
Osoby poddane badaniu	**Respondenci nauczyciele akademiccy**		**Respondenci kadra administracyjna**		**Respondenci studenci (różne kierunki)**	
Odpowiedź	*liczba wskazań*	*udział procentowy*	*liczba wskazań*	*udział procentowy*	*liczba wskazań*	*udział procentowy*
bardzo niska	0	0%	0	0%	9	1,8%
niska	6	1,2%	0	0%	35	7%
przeciętna	214	42,8%	129	25,8%	195	39%
wysoka	235	47%	356	71,2%	250	50%
bardzo wysoka	45	9%	15	3%	11	2,2%
	500	**100%**	**500**	**100%**	**500**	**100%**

18. Czy zdarza się Państwu przekazywać informacje dotyczące, danych, korespondencji, haseł itd. innym użytkownikom za pośrednictwem telefonu?

(w polu proszę wstawić znak „X")

TAK	**NIE**

Rozkład odpowiedzi respondentów w kwestionariuszu ankiety dla nauczycieli akademickich, kadry administracyjnej, studentów (różne kierunki):

Odpowiedzi badanych osób *Przekazywanie danych, korespondencji, haseł za pośrednictwem telefonu*						
Osoby poddane badaniu	**Respondenci nauczyciele akademiccy**		**Respondenci kadra administracyjna**		**Respondenci studenci (różne kierunki)**	
Ocena	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***	***liczba wskazań***	***udział procentowy***
TAK	0	0%	0	0%	22	4,4%
NIE	500	100%	500	100%	478	95,6%
	500	**100%**	**500**	**100%**	**500**	**100%**

19. Czy przechowują Państwo na pamięciach zewnętrznych dane i wydruki informacji przekazywanych w systemie informacyjnym?

(w polu proszę wstawić znak „X")

TAK	**NIE**

Rozkład odpowiedzi respondentów w kwestionariuszu ankiety dla nauczycieli akademickich, kadry administracyjnej, studentów (różne kierunki):

Odpowiedzi badanych osób *Przechowywanie na pamięciach zewnętrznych danych i wydruków informacji przekazywanych w systemie informacyjnym*

Osoby poddane badaniu	Respondenci nauczyciele akademiccy		Respondenci kadra administracyjna		Respondenci studenci (różne kierunki)	
Ocena	*liczba wskazań*	*udział procentowy*	*liczba wskazań*	*udział procentowy*	*liczba wskazań*	*udział procentowy*
TAK	467	93,4%	496	99,2%	492	98,4%
NIE	33	6,6%	4	0,8%	8	1,6%
	500	**100%**	**500**	**100%**	**500**	**100%**

20. Co chcieliby Państwo zmienić, aby zwiększyć bezpieczeństwo systemu informacyjnego w uczelni wyższej?

***1*……..**

***2*……..**

***3*……..**

***4*……..**

***5*……..**

(proszę o wypełnienie metryczki dotyczącej Państwa funkcji pełnionej w uczelni wyższej)

Metryczka respondenta: Nauczyciele akademiccy

(w polu proszę wstawić znak „X")

Lp.	*Nauczyciele akademiccy*	
1	*Wiek*	*…….lat*
2	*Płeć*	**kobieta** / **mężczyzna**
3	*Wykształcenie*	prof. / hab. / dr / mgr
4	*Staż pracy*	*…….lat*
5	*Staż pracy na uczelni wyższej*	*…….lat*

Metryczka respondenta: Kadra administracyjna

(w polu proszę wstawić znak „X”)

Lp.	*Kadra administracyjna*	
1	*Wiek*	*…….lat*
2	*Płeć*	**kobieta** **mężczyzna**
3	*Wykształcenie*	mgr / lic. / średnie / zasadnicze
4	*Staż pracy*	*…….lat*
5	*Staż pracy na uczelni wyższej*	*…….lat*

Metryczka respondenta: Studenci

(w polu proszę wstawić znak „X”)

Lp.	*Studenci*	
1	*Wiek*	*…….lat*
2	*Płeć*	**kobieta** **mężczyzna**
3	*Stopień*	**pierwszy** / **drugi** / **jedno-lite mgr**
4	*Forma kształcenia*	**stacjonarne** **niestacjonarne**

Załącznik 2

Kwestionariusz
do przeprowadzenia wywiadów z ekspertami

1. Temat badań: Bezpieczeństwo systemu informacyjnego organizacji publicznej na przykładzie uczelni wyższej
2. Cel badań: zebranie i opracowanie opinii ekspertów mających na celu weryfikację przyjętej hipotezy, konieczność wdrożenia zmian w bezpieczeństwie systemu informacyjnego w uczelni wyższej, mających za zadanie poprawić skuteczność ochrony informacji.
3. Teren badań: publiczna uczelnia wyższa.
4. Zakres problemowy badań: prośba skierowana o udzielenie wywiadu eksperckiego w ramach wsparcia badań wiedzą ekspercką i doświadczeniem zawodowym.

Kwestionariusz nakierowany jest na poznanie opinii użytkowników w zakresie bezpieczeństwa systemu informacyjnego w uczelni wyższej. Zebrane wyniki posłużą określeniu poziomu bezpieczeństwa systemu informacyjnego organizacji publicznej na przykładzie uczelni wyższej. Proszę Panią/Pana o udzielenie w niniejszym wywiadzie rzetelnych odpowiedzi.

- *Czy Pani/Pana zdaniem obecna organizacja i zasady użytkowania systemu informacyjnego w uczelni wyższej są odpowiednie do współczesnych potrzeb?*
- *Czy według Pani/Pana obecny obieg informacji w uczelni wyższej w pełni umożliwia sprawne oraz skuteczne zarządzanie w uczelni wyższej?*
- *Jakie Pani/Pana zdaniem zmiany w organizacji i funkcjonowaniu obiegu informacji w uczelni wyższej wpłynęły by na zwiększenie efektywności zarządzania?*
- *Jakie Pani/Pana zdaniem występują zagrożenia bezpieczeństwa systemu informacyjnego w uczelni wyższej?*
- *Jakie Pani/Pana zdaniem uwarunkowania wpływają na bezpieczeństwo systemu informacyjnego w uczelni wyższej?*

- *Jakie Pani/Pana zdaniem należy wprowadzić zmiany w bezpieczeństwie systemu informacyjnego w uczelni wyższej, aby poprawić skuteczność ochrony informacji?*

Serdecznie dziękuję za pomoc i współpracę oraz poświęcony czas

Mgr Agnieszka Gajewska

Sprawozdanie

z badań opinii ekspertów dotyczące problematyki bezpieczeństwa systemu informacyjnego organizacji publicznej na przykładzie uczelni wyższej

1. Temat badań: Bezpieczeństwo systemu informacyjnego organizacji publicznej na przykładzie uczelni wyższej;

2. Metody badań: metoda oceny ekspertów;

3. Cel badań: zebranie i opracowanie opinii ekspertów mających na celu weryfikację przyjętej hipotezy, konieczność wdrożenia zmian w bezpieczeństwie systemu informacyjnego w uczelni wyższej, mających za zadanie poprawić skuteczność ochrony informacji;

4. Opis przebiegu badań: Metoda oceny eksperta, poproszony o opinię został informatyk zatrudniony w uczelni wyższej;

W oparciu o pozyskane wypowiedzi można w odniesieniu do rozpatrywanych problemów sformułować następujące wnioski:

- *Czy Pani/Pana zdaniem obecna organizacja i zasady użytkowania systemu informacyjnego w uczelni wyższej są odpowiednie do współczesnych potrzeb?*

Obecna organizacja oraz zasady użytkowania systemu informacyjnego w uczelni wyższej nie są odpowiednie do współczesnych potrzeb. Konieczność jest zwiększenia bezpieczeństwa sprzętu wynoszonego na zewnątrz uczelni. Często widoczny jest brak zachowania ostrożności wśród osób używających taki sprzęt wynoszony poza mury uczelniane. Nie zostaje zachowana ostrożność podczas transportu a często także pozostaje w widocznym miejscu. Dużym problemem może być brak odpowiedniego przechowywania i użytkowania poza obszarem przetwarzania danych osobowych. Kluczowym także problemem jest brak świadomości użytkowników związany z procedurami posługiwania się systemem informacyjnym. Używanie prywatnych kont przekazu informacji i innych kanałów poza systemem w uczelni wyższej, które nie są przygotowane do tego, aby weryfikować

nadawcę. W uczelni wyższej zauważalny jest brak centralnego zarządzania, aktualnych wersji oprogramowania. W uczelni wyższej jest potrzeba wprowadzenia nowych rozwiązań systemowych jak również odpowiednich narzędzi informatycznych.

- *Czy według Pani/Pana obecny obieg informacji w uczelni wyższej w pełni umożliwia sprawne oraz skuteczne zarządzanie w uczelni wyższej?*

Obecny system obiegu informacji w uczelni wyższej nie w pełni umożliwia sprawne i skuteczne zarządzanie. Mnogość pracowników, studentów powoduje, ze informacje nie zawsze są dostarczone na czas. Czasami jest to wina bezpośrednio pracownika, braku kompetencji czy także opieszałości. Docierają one z opóźnieniem, ponieważ ktoś zapomniał treść wiadomości przekazać lub została ona przekazana do innej osoby często za pośrednictwem narzędzi to tego przeznaczonych. Widoczna jest mała odpowiedzialność za wykonywaną pracę lub roztargnienie czy przeczytanie pewnych wiadomości tylko wyrywkowo. Często bywa tak, że osoby zainteresowane czekają do ostatniej chwili a później same nie mają możliwości zmieścić się w terminie realizacji pewnych wytyczonych zadań, co powoduje zakłócenie prawidłowości i skuteczności zarządzania.

- *Jakie Pani/Pana zdaniem występują zagrożenia bezpieczeństwa systemu informacyjnego w uczelni wyższej?*

Zagrożenia bezpieczeństwa systemu informacyjnego w uczelni wyższej to m.in.: pożar, zalanie pomieszczeń, awarie sprzętu, awarie oprogramowania, niepożądane modyfikacje w systemie, manipulacja danymi osobowymi, ujawnienie osobom nieupoważnionym danych osobowych lub procedur, które zostały objęte ochroną przetwarzania, niewylogowanie się z systemu przed opuszczeniem stanowiska pracy lub brak wylogowania czy decyzja o zapamiętaniu przez system hasła, brak zamykania pomieszczeń, w których są komputery i włączone ekrany, modyfikacja danych, instalowanie oprogramowania, które może nosić miano wadliwego, pozostawienie nośników bez opieki, wydruków, pism, dokumentacji na biurkach zamiast pism wpiętych do segregatorów i zamkniętych na klucz w szafkach do tego przeznaczonych.

- *Jakie Pani/Pana zdaniem uwarunkowania wpływają na bezpieczeństwo systemu informacyjnego w uczelni wyższej?*

Jednym z uwarunkować, o których należy wspomnieć jest wykształcona świadomość pracownikowi i studentów w zakresie systemu, jak należy się nim posługiwać, jakie są niebezpieczeństwa, które powodują zagrożenia. Niedostosowanie się użytkowników do procedur wynikających z bezpiecznego korzystania z systemów informacyjnych i narzędzi informatycznych. Ważną rolę pełnią także finanse, którymi dysponuje uczelnia, jako cała organizacja i poszczególne jednostki organizacyjne, jakie można przeznaczyć na zakup nowych komputerów, oprogramowania, zabezpieczenia.

- *Jakie Pani/Pana zdaniem należy wprowadzić zmiany w bezpieczeństwie systemu informacyjnego w uczelni wyższej, aby poprawić skuteczność ochrony informacji?*

Poprawa skuteczności ochrony informacji i bezpieczeństwa systemu informacyjnego w uczelni wyższej polegać powinna na udoskonaleniu obecnego systemu informacyjnego w dodatkowe zabezpieczenia. Ważną kwestią jest zwiększenie kontroli pracowników.

Załącznik 3

Arkusz obserwacji

bezpośredniej organizacji i funkcjonowania publicznej uczelni wyższej

1. Temat badań: *B*ezpieczeństwo systemu informacyjnego organizacji publicznej na przykładzie;

2. Metody badawcze: obserwacja uczestnicząca;

3. Cel badań: sprawdzenie wewnętrznego i zewnętrznego obiegu informacji w uczelni wyższej oraz ocena bezpieczeństwa systemu informacyjnego w uczelni wyższej;

4. Opis przebiegu badań: badania przeprowadzone metodą obserwacji uczestniczącej wśród badanych grup respondentów;

Dzięki obserwacji uczestniczącej jest możliwość wnikliwego rozpoznania środowiska w uczelni wyższej i jego zasady funkcjonowania.

Wyniki obserwacji dały możliwość na sformułowanie wniosków a mianowicie:

- Struktura organizacyjna, brak kontroli użytkowników systemu informacyjnego przez władze uczelniane, brak nowego sprzętu, oprogramowania, przypisywanie uprawnień do osób, które nie maja takich zadań w swoim zakresie obowiązków, nadmierna ilość powierzonych zadań dla administratora danych, który jest informatykiem, niedostosowany czas pracy do pozostałych użytkowników systemu, zbyt duża ilość systemów we wszystkich komórkach organizacyjnych.
- Wewnętrzne zagrożenia dla bezpieczeństwa informacyjnego, pozostawienie pamięci zewnętrznych z danymi bez opieki w miejscach ogólnie dostępnych dla osób także nieupoważnionych, pozostawienie dokumentów z danymi na widoku w miejscach nieprzystosowanych do przechowywania dokumentacji, pozostawienie otwartych pomieszczeń, do których mają dostęp inne osoby do tego nieupoważnione, pozostawienie komputerów z danymi na ekranie, nie wylogowanie się z systemów, zapisywanie haseł w systemie z myślą, że nie trzeba będzie później wpisywać jednakże taki dostęp jest szybki dla hakerów, nieumyślne ujawnienie niedanych osobom trzecim, najczęściej takie sytuacje podyktowane są brakiem wiedzy, świadomości z zagrożenia, korzystanie z poczty indywidualnej, elektronicznej przez pracowników i studentów kształcących się w uczelni wyższej, nieświadome zlecenia wydruków dokumentów, pism, wśród nauczycieli akademic-

kich czy kadry administracyjnej czy pozostawienie takiej dokumentacji na drukarce, skanerze znajdującym się w innych pomieszczeniach, do których maja dostęp inne osoby.

- Zewnętrzne zagrożenia dla bezpieczeństwa informacyjnego, przekazywanie informacji za pośrednictwem telefonu, nie w pełni weryfikując prawdziwość osoby dzwoniącej i chcącej zasięgnąć informacji, udostępnienie urządzeń przenośnych z danymi na nich zapisanymi innym osobom nie koniecznie do tego uprawnionym, ujawnienie haseł do systemów wewnętrznych działających w uczelni wyższej, korzystanie z urządzeń przenośnych z dostępem do sytemu na zewnątrz uczelni wyższej.