AKADEMIA KALISKA

RADA DYSCYPLINY NAUK O BEZPIECZEŃSTWIE

ROZPRAWA DOKTORSKA

TEMAT

KONCEPCJA SYSTEMU BEZPIECZEŃSTWA WYMIANY INFORMACJI W PAŃSTWOWEJ STRAŻY POŻARNEJ

Opracował:

mgr inż. Andrzej Bartkowiak

Kierownik naukowy:

prof. dr hab. inż. Jarosław Wołejszo

KALISZ

maj 2023

Spis treści

STRESZCZENIE

Rozprawa doktorska pod tytułem „Koncepcja systemu bezpieczeństwa wymiany informacji w Państwowej Straży Pożarnej" w zamierzeniu jej autora dotyczyła identyfikacji i poznaniu istniejącego w Państwowej Straży Pożarnej systemu informacyjnego oraz występujących w nim zagrożeń, mankamentów i słabości. Następnie autor przedstawia autorską, możliwą do wprowadzenia koncepcję zmian w jego funkcjonowaniu, w celu usprawnienia działania całej formacji Państwowej Straży Pożarnej jako organizacji zhierarchizowanej.

W ramach niniejszej dysertacji została dokonana wnikliwa i precyzyjna analiza zasad funkcjonowania organizacji Państwowej Straży Pożarnej jako instytucji typowo zhierarchizowanej. Zbadano i zaprezentowano także otoczenie (zarówno wewnętrzne, jak i zewnętrzne) w jakim ta instytucja funkcjonuje. Przedstawiono wnikliwie definicję i rolę informacji oraz jej znaczenie dla sprawnego działania całego systemu informacyjnego, z uwzględnieniem zagrożeń na jakie narażony jest ten system. Zwrócono szczególną uwagę na skutki zakłóceń w procesie obiegu informacji. Jednocześnie zaproponowano szereg usprawnień odnośnie do polepszenia bezpieczeństwa istniejącego systemu informacyjnego z uwzględnieniem innowacyjnych rozwiązań w obszarze organizacyjnym, technicznym i funkcjonalnym.

Odpowiednio do przedmiotu oraz celu badań, główny problem badawczy dysertacji został określony pytaniem: *Jakie zmiany wprowadzić w systemie bezpieczeństwa wymiany informacji w organizacji publicznej jaką jest Państwowa Straż Pożarna, tak aby poprawić skuteczność bezpieczeństwa obiegu informacyjnego?*

Zasadniczym motywem, dla którego autor podjął się napisania niniejszej rozprawy doktorskiej były zawodowe doświadczenia podczas wieloletniej służby w Państwowej Straży Pożarnej, na różnych stanowiskach w jej strukturach i chęć przełożenia tych doświadczeń na poprawę skuteczności funkcjonowania jednej z najważniejszych formacji w systemie bezpieczeństwa państwa polskiego poprzez usprawnienie bezpieczeństwa systemu informacyjnego i obiegu informacji. Dotychczasowe doświadczenia związane z przepływem informacji, dostrzeżone niedoskonałości i braki w funkcjonującym systemie informacyjnym Państwowej Straży Pożarnej, zdaniem autora, wymagają wprowadzenia usprawnień w celu poprawy jego skuteczności, wyeliminowania zakłóceń w jego funkcjonowaniu oraz zapewnienia sprawnego przekazu informacji na wszystkich szczeblach hierarchii służbo-

wej. Opierając się na własnych doświadczeniach zawodowych, popartych wnikliwą analizą literatury przedmiotu autor doszedł do przekonania, że możliwe jest zaproponowanie zmian polegających na usprawnieniu bezpieczeństwa systemu informacyjnego Państwowej Straży Pożarnej. W konsekwencji ma poprawić to obieg informacji, jakość samej informacji w organizacji oraz wyeliminować wszelkie szumy komunikacyjne.

Dysertacja składa się z wstępu i zakończenia oraz czterech zasadniczych rozdziałów merytorycznych: Rozdział 1 Podstawy metodologiczne badań; Rozdział 2 Podstawy zarządzania bezpieczeństwem systemu informacyjnego w instytucjach publicznych; Rozdział 3 Zagrożenia bezpieczeństwa systemu informacyjnego na przykładzie Państwowej Straży Pożarnej; Rozdział 4 Koncepcja bezpieczeństwa systemu informacyjnego w Państwowej Straży Pożarnej.

W rozdziale pierwszym przedstawione zostały kwestie przedmiotu oraz celu badań naukowych. Nakreślony został problem badawczy, jak również hipotezy robocze oraz hipotezy szczegółowe. Przybliżone zostały również metody empiryczne i teoretyczne, techniki oraz narzędzia badawcze jakimi posługiwał się autor podczas swoich badań. Omówiono szczegółowo obszar badań, a także scharakteryzowano próbę badawczą, która została poddana tym badaniom.

W drugim rozdziale przedstawiona została teoria bezpieczeństwu systemu informacyjnego w instytucjach publicznych, z uwzględnieniem kontekstu teoretycznego i prawnego. W części tej określona została między innymi definicja informacji, ze szczególnym zaznaczeniem, czym jest bezpieczeństwo informacji dla współczesnych organizacji. Ponadto omówiono także znaczenie systemów bezpieczeństwa informacyjnego w aspekcie zapewnienia bezpieczeństwa państwa. Zaprezentowano środki techniczne i organizacyjne mające wpływ na bezpieczeństwo informacji w organizacji. W aspekcie prawnym przybliżono obowiązujące akty normatywne wraz z normami i innymi regulacjami powszechnie obowiązującymi. Następnie przedstawiono diagnozę systemu informacyjnego funkcjonującego w instytucjach państwowych z ujęciem zarządzania bezpieczeństwem informacyjnym w organizacji.

W rozdziale trzecim nakreślone zostały zagrożenia bezpieczeństwa systemu informacyjnego na przykładzie instytucji publicznej jaką jest Państwowa Straż Pożarna. Autor przedstawił aspekty systemu bezpieczeństwa oraz jego strategię, z uwzględnieniem norm i standardów bezpieczeństwa systemu informacyjnego, jakie powinny obowiązywać w instytucji państwowej. Dokonana została charakterystyka zagrożeń i ograniczeń bezpie-

czeństwa systemu informacyjnego w Państwowej Straży Pożarnej, wynikająca ze specyfiki jej działalności oraz licznego grona użytkowników.

Ostatni, czwarty rozdział stanowi empiryczną część pracy, obejmującą badania własne autora, które pomogły mu w opracowaniu własnej, nowatorskiej koncepcji bezpieczeństwa systemu informacyjnego w Państwowej Straży Pożarnej. Twórca nakreślił w niej kierunki zmian w funkcjonowaniu i organizacji systemu informacyjnego na poziomach organizacyjnym, technicznym i funkcjonalnym w celu poprawy jego bezpieczeństwa.

Rozprawa doktorska stanowi swoiste zestawienie i przegląd wiedzy z zakresu omawianej tematyki oraz jest obszernym zbiorem wyczerpujących treści odnoszących się do systemu informacyjnego. Przeprowadzona analiza literatury pozwoliła na stworzenie pracy o charakterze zwartym, nowatorskim i wyczerpującym główne założenia badawcze.

SUMMARY

The doctoral dissertation entitled „The concept of a security system for information exchange in the State Fire Service" was intended by its author to identify and learn about the information system existing in the State Fire Service and its threats, shortcomings and weaknesses. Then, the author presents an original, possible to introduce concept of changes in its functioning in order to improve the operation of the entire State Fire Service formation as a hierarchical organization.

As part of this dissertation, an in-depth and precise analysis of the principles of functioning of the State Fire Service organization as a typically hierarchical institution was made. The environment (both internal and external) in which the institution operates was also examined and presented. The definition and role of information and its importance for the efficient operation of the entire information system, including the threats to which this system is exposed, were thoroughly presented. Particular attention was paid to the effects of disruptions in the process of information circulation. At the same time, a number of improvements were proposed to improve the security of the existing information system, taking into account innovative solutions in the organizational, technical and functional areas.

According to the subject and purpose of the research, the main research problem of the dissertation was defined with the question: What changes should be introduced in the information exchange security system in a public organization such as the State Fire Service, so as to improve the effectiveness of information circulation security?

The main motive for which the author undertook to write this doctoral dissertation was professional experience during many years of service in the State Fire Service, in various positions in its structures, and the desire to translate these experiences into improving the effectiveness of one of the most important formations in the security system of the Polish state by improving security information system and information circulation. The previous experience related to the flow of information and the perceived imperfections and deficiencies in the functioning information system of the State Fire Service, according to the author, require improvements to improve its effectiveness, eliminate disruptions in its functioning and ensure efficient transfer of information at all levels of the service hierarchy. Based on his own professional experience, supported by a thorough analysis of the literature on the subject, the author came to the conclusion that it is possible to propose changes to improve the security of the information system of the State Fire Ser-

vice.

As a consequence, it is supposed to improve the flow of information, the quality of the information itself in the organization and eliminate all communication noise.

The dissertation consists of an introduction and conclusion as well as four substantive chapters: Chapter 1 Methodological basis of research; Chapter 2 Fundamentals of information system security management in public institutions; Chapter 3 Threats to the security of the information system on the example of the State Fire Service; Chapter 4 The concept of information system security in the State Fire Service.

The first chapter presents the subject and purpose of scientific research. The research problem was outlined, as well as working hypotheses and detailed hypotheses. Empirical and theoretical methods, techniques and research tools used by the author during his research were also presented. The area of research was discussed in detail, and the research sample that was subjected to this research was characterized.

The second chapter presents the theory of information system security in public institutions, taking into account the theoretical and legal context. This part defines, among others, the definition of information, with particular emphasis on what information security means for modern organizations. In addition, the importance of information security systems in the aspect of ensuring state security was also discussed. Technical and organizational measures affecting information security in the organization were presented. In the legal aspect, the applicable normative acts were approximated together with standards and other generally applicable regulations. Then, a diagnosis of the information system functioning in state institutions is presented, including information security management in the organization.

In the third chapter, threats to the security of the information system are outlined on the example of a public institution such as the State Fire Service. The author presented aspects of the security system and its strategy, taking into account the norms and standards of information system security that should apply in a state institution. The characteristics of threats and limitations of the security of the information system in the State Fire Service, resulting from the specificity of its activity and a large group of users, was made.

The last, fourth chapter is the empirical part of the work, covering the author's own research, which helped him to develop his own, innovative concept of information system security in the State Fire Service. In it, the creator outlined the directions of changes in the

functioning and organization of the information system at the organizational, technical and functional levels in order to improve its security.

The doctoral dissertation is a specific summary and review of knowledge in the field of the discussed subject and is an extensive collection of exhaustive content relating to the information system. The analysis of the literature allowed for the creation of a compact, innovative work that exhausts the main research assumptions.

Wstęp

Elementem bezpieczeństwa publicznego kraju jest bezpieczeństwo przeciwpożarowe oraz zapobieganie skutkom innych miejscowych zagrożeń. Państwowa Straż Pożarna jest jednym z podmiotów tego systemu realizującym zadania w ogólnym systemie bezpieczeństwa państwa i porządku publicznego.

Państwowa Straż Pożarna jest zawodową, umundurowaną i wyposażoną w specjalistyczny sprzęt formacją, przeznaczoną do walki z pożarami, klęskami żywiołowymi i innymi miejscowymi zagrożeniami. Centralnym organem administracji rządowej Państwowej Straży Pożarnej jest jej Komendant Główny, podległy ministrowi spraw wewnętrznych i administracji. Komendant Główny jest przełożonym wszystkich strażaków pełniących służbę w Państwowej Straży Pożarnej.

W wyniku przekształceń istniejących struktur ochrony przeciwpożarowej zgodnie z ustawą z dnia 24 sierpnia 1991 roku o Państwowej Straży Pożarnej, tworzą ją następujące jednostki organizacyjne:

komenda główna

szesnaście komend wojewódzkich,

- 335 komend powiatowych (miejskich);
- 510 jednostek ratowniczo-gaśniczych oraz 5 szkolnych;
- 5 szkół Państwowej Straży Pożarnej, w tym Szkoła Główna Pożarnicza w Warszawie, 2 szkoły aspirantów Państwowej Straży Pożarnej w Poznaniu i Krakowie, Szkoła Podoficerska w Bydgoszczy i Centralna Szkoła Państwowej Straży Pożarnej w Częstochowie;
- Centralne Muzeum Pożarnictwa w Mysłowicach;
- Centrum Naukowo-Badawcze Ochrony Przeciwpożarowej w Józefowie.

Zakres zadań tej formacji wynika z powyższej ustawy o Państwowej Straży Pożarnej i należy do nich między innymi:

- rozpoznawanie zagrożeń pożarowych i innych miejscowych zagrożeń;
- organizacja i prowadzenie akcji ratowniczych w czasie pożarów, klęsk żywiołowych lub likwidacji miejscowych zagrożeń;
- wykonywanie pomocniczych specjalistycznych czynności ratowniczych w czasie klęsk żywiołowych lub likwidacji miejscowych zagrożeń przez inne służby ratownicze;

– szkolenie kadr na potrzeby Państwowej Straży Pożarnej i innych jednostek ochrony przeciwpożarowej oraz powszechnego systemu ochrony ludności;
– nadzór nad przestrzeganiem przepisów przeciwpożarowych;
– prowadzenie prac naukowo-badawczych w zakresie ochrony przeciwpożarowej oraz ochrony ludności;
– współdziałanie ze strażami pożarnymi i służbami ratowniczymi innych państw;

Całokształt działań Państwowej Straży Pożarnej skupia się w ramach Krajowego Systemu Ratowniczo-Gaśniczego. Krajowy System Ratowniczo-Gaśniczy jest zespołem przedsięwzięć organizacyjnych, szkoleniowych, materiałowo-technicznych i finansowych obejmujących prognozowanie, profilaktykę, rozpoznawanie i zwalczanie pożarów, klęsk żywiołowych, miejscowych zagrożeń oraz organizację i kierowanie działaniami ratowniczymi, skupiających się w uporządkowanej wewnętrznie strukturze jednostki ochrony przeciwpożarowej w celu ratowania życia, zdrowia, mienia i środowiska. Centralnym organem administracji rządowej w sprawach organizacji Krajowego Systemu Ratowniczo-Gaśniczego oraz ochrony przeciwpożarowej jest Komendant Główny Państwowej Straży Pożarnej. Do niego należy m.in. kierowanie systemem. Jego działania nadzorowane są przez ministra spraw wewnętrznych i administracji, który odpowiada za realizację polityki państwa w zakresie ochrony przeciwpożarowej oraz pełni nadzór nad funkcjonowaniem Krajowego Systemu Ratowniczo-Gaśniczego. Na podstawie zawartych porozumień system wspomagają inne służby, inspekcje i straże: Policja, Straż Graniczna, Państwowa Inspekcja Ochrony Środowiska, Państwowa Agencja Atomistyki, Stacje Ratownictwa Górskiego, Morska Służba Poszukiwania i Ratownictwa. Wśród organizacji pozarządowych w systemie znajdują się: Górskie Ochotnicze Pogotowie Ratunkowe, Wodne Ochotnicze Pogotowie Ratunkowe, Związek Harcerstwa Polskiego, Polska Misja Medyczna, Polski Związek Alpinizmu i Tatrzańskie Ochotnicze Pogotowie Ratunkowe.

Zgodnie z właściwością terytorialną Krajowy System Ratowniczo-Gaśniczy tworzą oraz koordynują jego funkcjonowanie, następujące organy władzy:
– wójt (burmistrz lub prezydent miasta) w zakresie zadań ustalonych przez wojewodę;
– starosta, który określa zadania i kontroluje wykonywanie zadań na obszarze powiatu, a w sytuacjach nadzwyczajnych zagrożeń życia, zdrowia, środowiska i mienia zarządza systemem przy pomocy powiatowego zespołu reagowania kryzysowego;

– wojewoda, który określa zadania i kontroluje ich wykonanie na obszarze województwa, a w sytuacjach nadzwyczajnych zagrożeń życia, zdrowia, środowiska i mienia zarządza systemem przy pomocy wojewódzkiego zespołu zarządzania kryzysowego.

W Państwowej Straży Pożarnej struktura systemu obejmuje trzy poziomy działania. Na terenie kraju organizatorem i koordynatorem kierowniczym jest Komendant Główny Państwowej Straży Pożarnej, który wykonuje swoje zadania na poziomie krajowym, następnie odpowiednio na terenie województwa – komendant wojewódzki i na terenie powiatu – komendant powiatowy/miejski.

Reasumując, Państwowa Straż Pożarna jest bazą, na której opiera się Krajowy System Ratowniczo-Gaśniczy wraz ze swoim zapleczem kadrowym i logistycznym. Według danych Państwowej Straży Pożarnej, działania w tym systemie obejmują około 95% wszystkich zdarzeń w kraju wymagających szybkiej organizacji działań ratowniczych.

Wykonując swoje zadania Państwowa Straż pożarna jako instytucja publiczna posiada swój system bezpieczeństwa wymiany informacji. Z wieloletniej obserwacji autora zachowań wśród klientów oraz kadry pracowniczej można zaobserwować trudności i problemy, które bez wątpienia mają wpływ na bezpieczeństwo obiegu informacji wewnątrz instytucji. Autor korzystając z własnych przemyśleń, nowych poznawczych horyzontów oraz wnikliwej analizy literatury przedmiotu podejmie się próby zaprezentowania koncepcji zmian w obszarze bezpieczeństwa obiegu informacji.

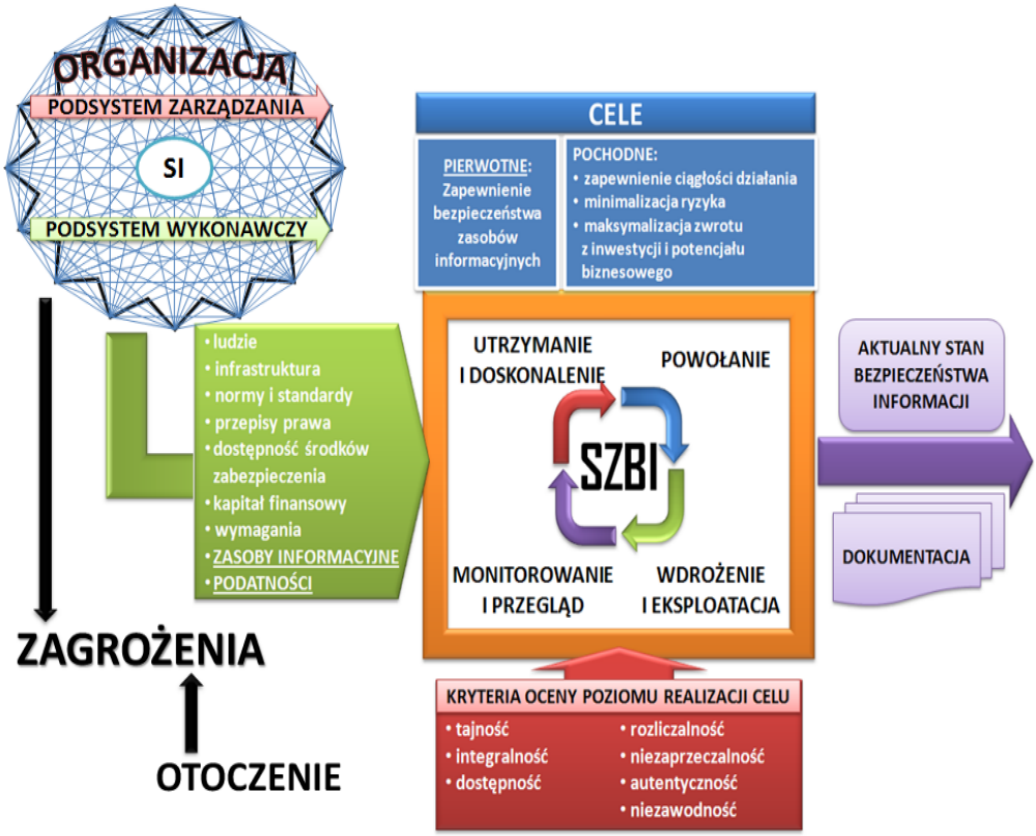
Realizacja coraz większej liczby zadań postawionych przed administracją państwa, związana jest z koniecznością wykorzystania nowoczesnych technologii. Instytucje realizujące zadania publiczne korzystają z szeregu różnych, często skomplikowanych, systemów teleinformatycznych, co wymaga przetwarzania zbiorów danych. Instytucje rządowe i samorządowe, to organizacje przetwarzające najbardziej szeroki zakres informacji. Mając na uwadze rosnące znaczenie systemów informacyjnych instytucji publicznych, celowym wydaje się podjęcie badań związanych z systemem zarządzania bezpieczeństwem informacji. W Państwowej Straży Pożarnej przetwarzane są również informacje niejawne oraz gromadzą są dane archiwalne. Bezpieczeństwo informacji z racji ilości, różnorodności oraz ważności realizowanych przez straż zadań jest ważna dla całego społeczeństwa.

Zwiększona ilość informacji, rozwój informatyzacji, ułatwienie dostępu do danych, usprawnienie procesów przekazywania lub pobierania ich znacznych ilości w niewielkich jednostkach czasu, rozwój technologii przechowywania informacji i wiele innych czynników przyczyniło się do wzrostu zainteresowania systemami zarzą-

dzania bezpieczeństwem informacji. Podejście to pozwala organizacjom odpowiednio przygotować się na zakłócenia związane z brakiem dostępności i integralności lub utratą poufności danych oraz wiele innych czynników.

Zapewnienie bezpieczeństwa systemu informacyjnego w organizacji publicznej jest wysoce cenione, gdyż stanowi o sile jednostki we współczesnej rzeczywistości. Kierownik każdej jednostki winien propagować politykę bezpieczeństwa informacyjnego wśród swojej kadry. Racjonalność w zarządzaniu informacją zaświadcza o wysokich kompetencjach menedżerskich oraz jest synonimem podążania jednostki za nieustannym rozwojem, który wywołuje ciągłą zmienność potrzeb.

Prawne aspekty wynikające z Konstytucji RP, Rozporządzenia Parlamentu Europejskiego i Rady UE 2016/679 z dnia 27 kwietnia 2016 r. (tzw. RODO) oraz Ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych ze zmianami przyczyniły się do zwiększenia uwagi na problem bezpieczeństwa danych osobowych w jednostkach organizacyjnych.



Źródło: P. Zaskórski, K. Szwarc, *Bezpieczeństwo zasobów informacyjnych determinantą informatycznych technologii zarządzania,* Zeszyty Naukowe Warszawskiej Wyższej Szkoły Informatyki Nr 9, Rok 7, 2013, s. 43

Rysunek 1-1
Model systemu zarządzania bezpieczeństwem informacji w organizacji.

Rozdział 1 PODSTAWY METODOLOGICZNE BADAŃ

1.1 UZASADNIENIE PODJĘCIA BADAŃ (SYTUACJA PROBLEMOWA)

W ramach rozprawy doktorskiej analizą zostanie objęty poziom bezpieczeństwa systemu informacyjnego w Państwowej Straży Pożarnej jako organizacji publicznej. Przeznaczenie Straży Pożarnej do celów zapewnienia bezpieczeństwa polskiemu społeczeństwu wymaga zapewnienia nie tylko odpowiedniej infrastruktury wraz z wykwalifikowaną kadrą pracowniczą, ale i stawia zadanie dla Komendanta Głównego utrzymania pełnego bezpieczeństwa systemu informacyjnego.

Dzisiejsza rzeczywistość zmusza do wnikliwej analizy poziomu bezpieczeństwa systemu informacyjnego w podmiotach sfery publicznej. Jest to konieczne, aby wzmacniać kanały informacji, które nie są należycie chronione, gdzie występuje brak kontroli nad przepływem wszelkiej informacji.

Jeżeli więc, w obszarach systemu informacyjnego w może występować zjawisko niekontrolowanego przepływu informacji, należy natychmiast wdrożyć środki zaradcze w tym zakresie. Nie ma jednak wątpliwości, że w każdej jednostce niezbędne jest podejmowanie decyzji w tradycyjnie ujmowanych czterech podstawowych obszarach procesu zarządzania tj. planowanie, organizowanie, motywowanie i kontrolowanie. Dotyczy to również sfery bezpieczeństwa systemu informacyjnego.

Dodatkowym czynnikiem determinującym stały wzrost zainteresowania tematyką bezpieczeństwa informacji są potrzeby dostosowywania organizacji do wymagań mających zastosowanie przepisów prawa i innych wymagań, których celem jest zapewnienie ochrony określonym grupom interesariuszy.

Autor w swojej pracy skupi się na systemie bezpieczeństwa informacji w organizacji przedstawiając „teorię problemu". Wskazana zostanie również istota systemu bezpieczeństwa informacji w organizacji Państwowej Straży Pożarnej, definiując pojęcia takie jak informacja czy bezpieczeństwo informacji. Przedstawione zostaną również prawne wymagania, co do bezpieczeństwa informacji oraz środki techniczne i organizacyjne mające wpływ na bezpieczeństwo informacji w organizacji publicznej. Istotną częścią będzie wskazanie elementów mających wpływ na zarządzanie bezpieczeństwem informacyjnym w organizacji, a także opisanie, czym jest ryzyko w zarządzaniu

bezpieczeństwem informacyjnym, jakie znaczenie ma przeprowadzanie audytów oraz jak powinno wyglądać prawidłowe wdrażanie systemu zarządzania bezpieczeństwem informacyjnym. Przedstawione zostaną zagadnienia organizacji publicznych ze wskazaniem cech charakterystycznych współczesnych organizacji i ich zasobów.

Dlatego przedmiotem dysertacji jest bezpieczeństwo systemu informacyjnego organizacji publicznej na przykładzie Państwowej Straży Pożarnej, które winno mieć przełożenie na właściwą organizację jej struktury poprzez skuteczne zarządzanie bezpieczeństwem informacyjnym. W ocenie badającego bezpieczeństwo systemu informacyjnego bez wątpienia ma istotny wpływ na zapewnienie bezpieczeństwa narodowego, a problematyka bezpieczeństwa systemu informacyjnego powinna być nadrzędnym celem w zarządzaniu, każdą organizacją. Złożoność procesu pozyskiwania, gromadzenia, utrzymywania, aktualizowania, przetwarzania, przesyłania i archiwizowania informacji wymaga szczególnych form postępowania na każdym jej etapie. Zdarza się, że nie wszystkim jednostkom to się w pełni udaje, często bezpieczeństwo sytemu informacyjnego ma charakter fragmentaryczny, który dotyczy tylko wybranych obszarów zarzadzania informacją. Bezpieczeństwo systemu informacyjnego powinno obejmować środowisko techniczne, informatyczne, system zarządzania, finanse, ekonomikę organizacji, zasoby ludzkie, otoczenie prawne i społeczne.

Swoje przemyślenia odnośnie do nowej koncepcji autor poprze przedstawioną analizą wyników przeprowadzonych badań na temat systemu bezpieczeństwa obiegu informacji, wskazując odpowiednie wnioski weryfikujące przyjęte hipotezy. Badanie poziomu bezpieczeństwa sytemu informacyjnego w straży pożarnej pozwoli ocenić jego rzeczywisty stan. Z uwagi na środowisko badanej jednostki publicznej uzyskane wyniki będą miały przełożenie na ogólną ocenę bezpieczeństwa tej struktury organizacyjnej i tym samym bezpieczeństwa narodowego. Posiadanie pełnej wiedzy o stanie bezpieczeństwa systemu informacyjnego w Państwowej Straży Pożarnej, w razie pewnych niedoskonałości uświadomi potrzebę zwiększenia działań prewencyjnych w tym zakresie.

Dlatego celem pracy jest znalezienie skutecznych rozwiązań, których zastosowanie wpłynęłoby z jednej strony na zwiększenie bezpieczeństwa systemu informacyjnego w omawianej organizacji publicznej, a z drugiej na poprawę, jakości wymiany informacji. Praca ma charakter poznawczy, ma skutkować wnikliwym zbadaniem i naukowym poszerzeniem wiedzy na temat systemu obiegu informacji w organizacji publicznej na przykładzie Państwowej Straży Pożarnej.

1.2 PRZEDMIOT i CEL BADAŃ

Przedmiotem badań niniejszej pracy jest *system bezpieczeństwa wymiany informacji w Państwowej Straży Pożarnej.*

Warto w tym miejscu podkreślić, że przedmiot badań w niniejszej dysertacji ze względu na jego strukturę posiada charakter interdyscyplinarny.

Natomiast w naukach społecznych cel badań należy percypować w sposób zróżnicowany ze względu na jego przedmiot lub przynależność do określonej dyscypliny. Cel badań społecznych postrzegany może być jako poznawczy, prognostyczny lub planistyczny[1].

W kontekście przedstawionego powyżej przedmiotu badań **celem niniejszej dysertacji** będzie:

1. Cel poznawczy: *identyfikacja zagrożeń i możliwych usprawnień w systemie bezpieczeństwa informacji w Państwowej Straży Pożarnej jako organizacji publicznej*.
2. Cel utylitarny: *opracowanie koncepcji bezpieczeństwa systemu obiegu informacji w organizacji publicznej jaką jest Państwowa Straż Pożarna.*

1.3 PROBLEM (PROBLEMY) BADAWCZY

Ze względu na przyjęty obszar i cel badań **głównym problemem badawczym** będzie odpowiedź na pytanie: *Jakie zmiany wprowadzić w systemie bezpieczeństwa wymiany informacji w organizacji publicznej jaką jest Państwowa Straż Pożarna, tak aby poprawić skuteczność bezpieczeństwa obiegu informacyjnego?*

Rozwiązanie powyższego głównego problemu badawczego wymaga uzyskania odpowiedzi na szereg **szczegółowych problemów**:

1. *Jak funkcjonuje system bezpieczeństwa wymiany informacji w teorii i praktyce?*
2. *Jak funkcjonuje system bezpieczeństwa wymiany informacji w organizacji publicznej jaką jest Państwowa Straż Pożarna?*
3. *Jaka powinna być koncepcja systemu obiegu informacji w Państwowej Staży Pożarnej, aby poprawić skuteczność jego funkcjonowania?*

[1] J. Sztumski, *Wstęp do metod i technik badań społecznych,* „Śląsk" Wydawnictwo Naukowe, 2010 r., s. 20–21.

1.4 HIPOTEZA ROBOCZA

Do tak przyjętego celu i głównego problemu badawczego, na podstawie obecnego stanu wiedzy oraz prognozowanych zmian można sformułować następującą hipotezę roboczą:

Założono, że obecny system informacyjny w organizacji publicznej jaką jest Państwowa Straż Pożarna nie w pełni chroni informacje pozyskiwane i przetwarzane przez tą formację. Ułatwienie dostępu do danych, usprawnienie procesów przekazywania lub pobierania ich znacznych ilości w niewielkich jednostkach czasu oraz rozwój technologii przechowywania informacji mają ogromne znaczenie na funkcjonowanie tej instytucji. Natomiast odpowiednio przebiegający proces wymiany informacji wpływa między innymi na prawidłowe wykonywanie zadań, przy założeniu, że najważniejszymi aspektami bezpieczeństwa informacji są: dostępność, poufność, niezawodność, integralność i autentyczność.

Obok głównej hipotezy autor postawił następujące szczegółowe hipotezy robocze, które są odpowiedzią na postawione wcześniej problemy badawcze szczegółowe:

Hipoteza 1: *Zakłada się, że bezpieczeństwo systemu informacji w Państwowej Straży Pożarnej regulowane jest pośrednio i bezpośrednio źródłami powszechnie obowiązującego prawa w Rzeczypospolitej Polskiej, do których należą między innymi: Konstytucja RP, ustawy, ratyfikowane umowy międzynarodowe, rozporządzenia, akty prawa miejscowego obowiązujące na obszarze działania organów, które je ustanowiły. System bezpieczeństwa wymiany informacji to strategia działania tej formacji w zakresie zapewniania właściwej ochrony pozyskiwanych i przetwarzanych informacji. W teorii strategia ta ma zapewnić ciągłe doskonalenie podjętych działań i procedur w celu optymalizacji ryzyk związanych z naruszeniem poufności danych. Natomiast w praktyce na strategię składają się wszystkie procedury, polityki, regulaminy i instrukcje bezpieczeństwa informacji, które są wdrożone w każdej jednostce organizacyjnej. Informacja jako zasób i narzędzie stanowi podstawę działalności analitycznej. Bez informacji i jej właściwego procedowania w systemie nie ma szans na właściwe, efektywne i szybkie wykorzystanie działalności analitycznej dla zwiększenia bezpieczeństwa państwa i obywateli, a bezpieczeństwo systemu informacyjnego świadczy o wysokim standardzie zarządzania jednostką organizacyjną.*

Hipoteza 2: *Zakłada się, że Państwowa Straż Pożarna jako instytucja odpowiedzialna za zapewnienie bezpieczeństwa obywatelom naszego Państwa gromadzi i przetwarza tylko niezbędna informacje w tym zakresie. Informacje te uzyskiwane są od „klientów”*

i instytucji, z którymi straż pożarna współpracuje. Informacje te przechowywane są w systemach informatycznych, dlatego bardzo ważne jest by prawidłowo funkcjonował system bezpieczeństwa wymiany informacji i każdy z pracowników tej instytucji powinien ją należycie chronić. Przypuszcza się natomiast, że jednym z najważniejszych potencjalnych źródeł zagrożeń dla bezpieczeństwa informacji w danej organizacji jest naruszanie przepisów chroniących te organizacje przez osoby, które posiadają dostęp do informacji. Występują zagrożenia w bezpieczeństwie sytemu informacyjnego dlatego, że dotychczasowe zabezpieczania informacji i procedury bezpieczeństwa informacyjnego nie są przez wszystkich użytkowników w należyty sposób przestrzegane. Do tego, występuje brak świadomości wśród niektórych użytkowników o skutkach łamania zasad korzystania z systemu informacyjnego i braku odpowiedzialności. Napotyka się również bariery oraz trudności powiązane bezpośrednio z wdrażaniem w życie ustawy o ochronie informacji niejawnych.

Ponadto zakłada się, że jako typowe zagrożenia systemu bezpieczeństwa obiegu informacji można wyodrębnić zagrożenia wewnętrzne i zewnętrzne powstające poza organizacją, w wyniku celowego lub przypadkowego działania ze strony osób trzecich. Do tych pierwszych zaliczyć możemy: zagrożenie utratą, uszkodzeniem danych lub brakiem możliwości obsługi z powodu błędu jak i przypadku; zagrożenie utratą lub uszkodzeniem poprzez celowe działania nieuczciwych użytkowników; zagrożenia fizyczne, w których szkoda jest spowodowana wypadkiem, awarią, lub innym nieprzewidzianym zdarzeniem losowym. Do zagrożeń zewnętrznych zaliczyć możemy: przestępstwa wykorzystujące komputer jako narzędzie; cyberterroryzm; utrata informacji związana z włamaniami komputerowymi, złośliwymi kodami i wirusami, szpiegostwem, sabotażem, czy też wandalizmem.

Hipoteza 3: *Zakłada się, że należy poprawić skuteczność obiegu informacji oraz zwiększyć efektywność zabezpieczeń informacji wewnątrz organizacji publicznej jaką jest Państwowa Straż Pożarna. Aby tego dokonać należałoby ujednolicić systemy teleinformatyczne na wszystkich poziomach organizacyjnych tej formacji oraz wprowadzić zmiany pod kątem organizacyjnym, technicznym i funkcjonalnym w zasadach użytkowania, funkcjonowania i organizacji systemu informacyjnego. Istotne jest wdrożenie i utrzymanie właściwego systemu zarządzania bezpieczeństwem informacji, który będzie umożliwiał ochronę wszystkich przetwarzanych informacji, jak również zapewniał ciągłość realizowanych procesów i zadań. Aby osiągnąć jak najwyższy stopień bezpieczeństwa informacji, należy w odpowiedni sposób przygotować zasoby organizacji, a następnie odpowiednio i odpowiedzialnie nimi zarządzać. Zakłada się, że niezbędne dla ochrony informacji*

w instytucji jest właściwie ułożenie i konsekwentne egzekwowanie polityki bezpieczeństwa informacji, co jest elementem decydującym o jej skuteczności, a systematyczny wielopłaszczyznowy nadzór zwiększa bezpieczeństwo informacji będących w obiegu.

1.5 METODY BADAWCZE

Na potrzeby opracowania niniejszej pracy, zostanie użytych szereg metod i technik badawczych, co jest potrzebą wynikającą ze złożoności rozpatrywanej problematyki.

Podając za J. Apanowiczem metoda badawcza to sposób pracy badawczej charakteryzujący się zarówno określonymi czynnościami postępowania (procedurą badawczą), jak i zastosowaniem odpowiednich narzędzi badawczych. Istota metody badawczej powinna zmierzać do skoordynowania sposobu postępowania z zakładanym celem badań[2].

T. Kotarbiński metodę badawczą przedstawia jako „*sposób systematycznie stosowany w danym przypadku z intencją zastosowania go także przy ewentualnym powtórzeniu analogicznego działania[3]". Natomiast w*edług M. Pelca metodę badawczą należy traktować jako „*narzędzie intelektualnego wsparcia badacza".[4]* Metoda badawcza poddawana modyfikacji i ulepszeniu przez badaczy staje się wartością dydaktyczną oraz przyczynia się do doskonalszego poznania rzeczywistości. Dobra metoda powinna zapobiegać błędom i przyczyniać się do poszerzania wiedzy. Zaś nowe badania powodują rozwój metod i jednocześnie przyczyniają się do korekty błędów[5].

Według J. Sztumskiego metodę badawczą można zdefiniować jako system założeń i reguł pozwalający na takie uporządkowanie praktycznej lub teoretycznej działalności, aby można było osiągnąć cel do jakiego się świadomie zmierza[6] i zaproponował następujący podział według:

- stopnia ogólności – zakres i powszechność stosowania metody badawczej.
- celu badania – metody badawcze służą różnym celom.
- przedmiotu badania – badane mogą być realnie i obiektywnie przedmioty istniejące lub też sposoby myślenia i tworów językowych.
- struktury poznania naukowego - polega na poznawaniu grup obiektów przyrodniczych, struktur społecznych, sposobów myślenia i syntezy języków naukowych.

[2] J. Apanowicz, *Metodologia ogólna*, Wyższa Szkoła Administracji i Biznesu, Gdynia, 2002 r., s. 60.
[3] T. Kotarbiński, *O pojęciu metody*, Wyd. PWN, Warszawa 1957, s. 667.
[4] M. Pelc, *Elementy metodologii badań naukowych*, Wyd. AON, Warszawa 2012, s. 49.
[5] B. Poskrobko *Metody badań naukowych z przykładami ich zastosowania*, Wydawnictwo Ekonomia i Środowisko, Białystok 2012 r., s. 48.
[6] J. Sztumski, *Wstęp do metod…*, op.cit, s. 60.

- charakteru nauk, w których są one stosowane – podział metod na metody nauk przyrodniczych i społecznych.[7]

Jak podaje E. Nowak metoda badawcza musi spełniać następujące wymogi:

- jasność – metoda musi być zrozumiała.
- jednoznaczność – powinno się stosować jednoznaczne sposoby i zasady.
- ukierunkowanie – musi mieć konkretny cel.
- skuteczność – powinna dążyć do osiągnięcia zamierzonego celu.
- owocność- oprócz dostarczenia pożądanych celów powinna dostarczać jeszcze inne, poboczne na rzecz tej samej lub innej dziedziny nauki.
- niezawodność – musi uzyskać zamierzone cele i rezultaty.
- ekonomiczność – powinna osiągnąć założone cele przy jak najmniejszych nakładach finansowych, zużyciu siły środków i czasu[8].

Zazwyczaj przy próbie rozwiązania problemu badawczego wybiera się jedną metodę jako główną a inne są metodami pomocniczymi[9].

Metoda badawcza i technika są ściśle powiązane z procesem badawczym. Metoda jest pojęciem szerszym niż technika i wskazuje na zakres i charakter prowadzonych badań. Technika badawcza to określone sposoby i umiejętność wykorzystania wybranych metod badawczych, czynności i operacji, które wpływają na poznanie właściwości przedmiotu badań.[10] Do technik badawczych można zaliczyć wszystkie dostępne narzędzia, środki, umiejętności i procedury stosowane w celu empirycznego zbadania założeń metodologicznych w pracy naukowej[11].

Wybrane techniki zastosowane w pracy naukowej powinny pomóc poznać opracowywany temat w sposób możliwie najszerszy i najdoskonalszy. Należy jednak pamiętać, że muszą być koniecznie dostosowane do badanej treści, gdyż mają zasadniczy wpływ na formułowane w pracy wnioski.

W niniejszej dysertacji autor zastosuje zarówno metody badawcze teoretyczne jak i empiryczne. Metody teoretyczne wpłyną na uzyskanie obszernego materiał badawczego. To pozwoli wyodrębnić składniki istotne w procesie badawczym, a następnie porównanie i

[7] J. Sztumski, *Wstęp do metod…,* op.cit., s. 45.
[8] E. Nowak, *Teoretyczne metody badawcze w naukach społecznych*, Obronność, Zeszyty Naukowe Wydziału Zarządzania i Dowodzenia Akademii Obrony Narodowej nr 2(6), 2013 r, s. 143.
[9] J. Apanowicz, *Metodologia ogólna*…, op.cit., s. 61.
[10] D. Nachmias, Frankfort-Nachmias C., *Metody badawcze w naukach społecznych*, Wydawnictwo Zysk i S-ka, Poznań, 2001 r., s. 21.
[11] F. Krzykała, *Metodologia badań i technik badawczych socjologii gospodarczej*, Wydawnictwo Akademii Ekonomicznej, Poznań, 2001 r., s. 40-41.

syntezę wyodrębnionych elementów składowych w celu uzyskania materiału niezbędnego do dalszych badań. Zastosowane metody badawcze umożliwią skonstruowanie merytorycznych wniosków na poszczególnych etapach procesu badawczego.

Proces badawczy w niniejszej pracy będą określały następujące metody:

- **teoretyczne**: abstrahowanie, analiza, synteza, uogólnienie, porównanie i analogia, wnioskowanie. Metody te będą stosowane podczas wszystkich etapów prowadzonych badań, a ich dobór jest dostosowany do charakteru problemu badawczego.
- **empiryczne**: obserwacja, badanie opinii techniką ankiety audytoryjnej, gdzie narzędziem badawczym jest kwestionariusz ankiety.

Metody teoretyczne w badaniach społecznych są konieczne do stosowania podczas analizy dokumentów, przy czym za dokumenty uznaje się każdy dowód ludzkiej działalności uchwytny materialnie (obraz, nagranie, wideo, fotografię, przedmiot, itp.). Jest to tzw. ujęcie dokumentu w szerokiej perspektywie. Natomiast w wąskiej perspektywie mamy do czynienia z pewnym typem unormowanej prezentacji pisemnej, jak np. sprawozdania, opisy statystyczne, transkrypcje wywiadów, itp.[12].

Czynności związane z różnorodnymi sposobami przygotowania i przeprowadzenia badań naukowych najczęściej dzielone są ze względu na rodzaj metody.

Analiza: autor dysertacji zastosuje tą metodę badawczą do myślowego rozłożenia przedmiotu badań na części, a następnie ich badania oddzielnie jako części poszczególnych zjawisk, w celu ich zbadania i wychwycenia istoty[13].

Analiza jest jedną z najważniejszych metod badawczych wykorzystywanych w naukach społecznych i innych dziedzinach nauki. Jest to proces systematycznego badania, rozkładu na części składowe i badania elementów w celu zrozumienia ich natury, funkcji i wzajemnych relacji. Analiza może być stosowana do różnych aspektów badania, w tym danych, tekstów, zjawisk społecznych, materiałów źródłowych i innych. Metoda analizy polega na dokładnym badaniu, ocenie i interpretacji danych lub materiałów w celu wydobycia informacji, odkrycia wzorców, zależności i znaczenia. Istnieje wiele różnych podejść i technik analizy, z których każda ma swoje własne zalety i zastosowania w zależności od kontekstu badawczego.

W metodologii wyróżnia się następujące typy analizy (rys. 1.1.)[14]:

[12] J. Sztumski, *Wstęp do metod…,* op.cit., s. 140-147.

[13] M. Cieślarczyk (red.), *Metody, techniki i narzędzia badawcze oraz elementy statystyki stosowane w pracach magisterskich i doktorskich*, Wyd. AON, Warszawa 2006, s. 46-47.

- *elementarna*, czyli analiza poszczególnych elementów całości w oderwaniu od siebie;
- *strukturalna*, czyli koncentracja na zbadaniu składu i struktury obiektów;
- *funkcjonalna* weryfikuje funkcje realizowane przez elementy obiektów;
- *przyczynowa,* skupiająca się na wskazaniu i badaniu zależności pomiędzy elementami składowymi;
- *logiczna*, czyli skupiająca się na stosunkach logicznych zachodzących pomiędzy elementami złożonego przedmiotu badań;
- *porównawcza,* umożliwiająca wykazanie wszelkich zmian i nieprawidłowości działania oraz odchyleń od przyjętych norm poprzez porównanie z faktami przyjętymi za wzorcowe bądź optymalne;
- *genetyczna,* badająca związki genetyczne;
- *matematyczna*, prowadzona w celu formalizacji wiedzy naukowej, czyli matematyzacji;
- *ilościowa*, której zadaniem jest opis faktów, zjawisk, procesów, a do jej przeprowadzenia potrzebne są różnego rodzaju tabele statystyczne;
- *jakościowa*, czyli dokonanie jakościowego opisu badanych faktów, zjawisk, procesów i zazwyczaj jest prowadzona z pominięciem wszelkich zawiłych zestawień liczbowych i obliczeń statystycznych;
- *ilościowo-jakościowa*, która jest połączeniem dwóch rodzajów analizy – analizy ilościowej i jakościowej; jest ona wymagana podczas badań empirycznych, gdyż nie istnieje taki przedmiot badań, który byłby wyłącznie określany ilościowo, czy jakościowo;
- *systemowa,* mogąca obejmować badanie całego systemu, jak i wyłącznie jego jednego aspektu, jak np.: strukturalnego, funkcjonalnego albo informacyjnego;
- *wartości,* obejmująca badanie funkcji badanego przedmiotu – organizacji, systemu. Koncentracja badacza skupia się na obniżeniu kosztów funkcji spełnianych przez badany przedmiot (koszt-efekt);
- *krytyka źródeł oraz krytyka piśmiennictwa* (literatury przedmiotu).

Metoda ta będzie zastosowana przede wszystkim do studiowania literatury przedmiotu, gdzie autor dysertacji zgromadzi i wyselekcjonuje niezbędne informacje zawarte

[14] J. Pieter, *Ogólna metodologia pracy naukowej,* Wydawnictwo Zakładu Narodowego im. Ossolińskich, Wrocław 1967, s. 127-130.; M. Cieślarczyk, (red.), *Metody, techniki*…,op. cit., s.47-48.

w literaturze i dokumentach normatywnych. Pozwoli to na istotne pogłębienie wiedzy w obszarze złożonej problematyki badawczej.

Autor dysertacji zastosuje analizę zarówno jako proces myślowy oraz metodę badawczą. Metoda ta zostanie wykorzystana jako analiza jakościowa i ilościowa. W przypadku analizy ilościowej sprowadzać się to będzie do opisu faktów, zjawisk i procesów, gdzie wykorzystywane będą tabele i wykresy. Analiza jakościowa pozwoli natomiast na dokonanie dokładnego opisu badanych zjawisk i faktów. Użycie tej metody przyczyni się do dokonania opisu badań, a także porównania ze sobą różnych danych zgromadzonych w procesie badań empirycznych. Przyczyni się to także do wskazania korelacji pomiędzy nimi jak i wyciągnięcie wniosków z analizowanych danych.
Będzie ona podstawą do sformułowania problemów badawczych szczegółowych oraz posłuży do sformułowania hipotez roboczych.

Źródło: M. Cieślarczyk (red.), *Metody, techniki i narzędzia badawcze oraz elementy statystyki stosowane w pracach magisterskich i doktorskich,* wyd. AON, Warszawa 2006, s. 46-47.

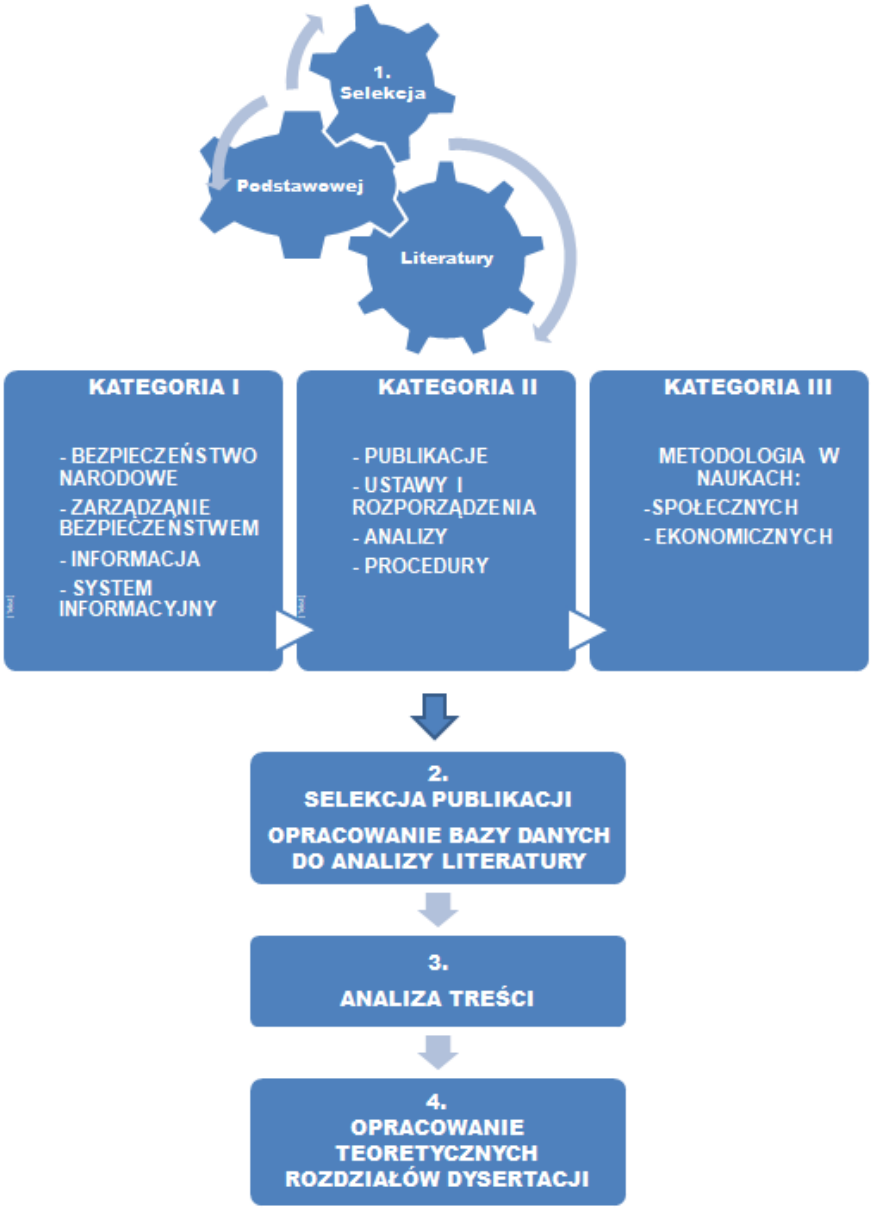
Rysunek 1-2 Typy analizy

Autor odwoła się również do tej metody podczas procesu systematyzowania przeglądu analizowanej literatury przedmiotu. Będzie to polegało na ustaleniu pewnej deklaracji rygoru doboru analizowanych pozycji literatury, co będzie miało na celu poznanie stanu wiedzy w danym obszarze oraz pozwoli na wskazanie ewentualnych niedoskonałości w obecnie funkcjonującym stanie rzeczy.

Autor zgromadzi i przeanalizuje pozycje, a następnie dokona podziału na trzy podstawowe grupy:

- opracowania teoretyczne dotyczące systemu obiegu informacji w organizacji publicznej;

- publikacje traktujące o bezpieczeństwie systemu obiegu informacji w organizacji publicznej. W tej kategorii literatury szczególną uwagę autor poświęci opracowaniom dotyczącym bezpieczeństwa systemu obiegu informacji w organizacji publicznej oraz dokumentom normatywnym zawierającym w swoich zapisach zagadnienia zbieżne z obszarem badań;
- publikacje poświęcone tematyce metodologii procesu prowadzenia badań naukowych. Na tym etapie procesu badawczego autor założy, że pogłębienie wiedzy ze wskazanego obszaru umożliwi właściwy wybór metod badawczych do rozwiązania poszczególnych problemów naukowych oraz opracowania uzyskanych wyników badań.



Źródło: W. Czakon, *Opracowanie własne na podstawie - Podstawy metodologii w naukach o zarządzaniu,* Wyd. Oficyna, Warszawa 2013 r., s. 52.

Rysunek 1-3 Proces krytycznej analizy literatury.

Analiza literatury przedmiotu będzie miała na celu poznanie stanu wiedzy w obszarze bezpieczeństwa systemu obiegu informacji w organizacji publicznej oraz wskazanie potencjalnych niedoskonałości w obecnie funkcjonującym obiegu tychże informacji. Selekcji publikacji (Etap 2, rys. 2.) autor dokona według następujących słów kluczowych: bezpieczeństwo, organizacje, organizacje publiczne, zarządzanie, bezpieczeństwo informacji, zarządzanie informacją, obieg informacji, badania, rozwój, bezpieczeństwo obiegu informacji, obronność, kierownik kancelarii, metodyka obiegu informacji, informacja niejawna, bezpieczny obieg informacji niejawnych. W ramach selekcjonowania literatury, w sposób ograniczony, czyli tzw. wstępnej analizy autor rozprawy będzie analizował: recenzje książek, ich wstępów i wniosków, w których zazwyczaj są zawarte interpretacje i syntetyczne wywody zawarte w publikacjach oraz poradniki, gdyż charakteryzują się one dyrektywnymi cechami oraz ograniczonym rygorem metodologicznej obiektywności.

Synteza jako metoda badawcza teoretyczna, stanowi spójność z analizą, a jej zadaniem jest łączenie wyodrębnionych składników przedmiotu badań w nową całość, co w konsekwencji prowadzi do wykrycia istotnych związków i właściwości[15]. Należy podkreślić w tym miejscu, że synteza nie jest jednak zwykłą odwrotnością analizy, gdyż wskazuje na nową jakość połączonych składowych poddanych analizie[16]. Odnosi się do procesu integracji, analizy i syntezy wyników badań pierwotnych w celu wyodrębnienia głównych tematów, wzorców, zależności i wniosków na podstawie istniejącej literatury naukowej lub innych źródeł informacji. Jest to ważne narzędzie w badaniach literaturowych, metaanalizach i syntezach systematycznych.

Metoda syntezy polega na przeglądzie, selekcji i analizie istniejących publikacji naukowych, artykułów, raportów lub innych materiałów badawczych. Następnie dokonuje się zintegrowanej analizy danych, w której porównuje się, łączy i syntetyzuje informacje z różnych źródeł w celu uzyskania całościowego spojrzenia na badane zagadnienie.
Przy odpowiednim podejściu i solidnym opracowaniu, metoda syntezy może dostarczyć wartościowych wniosków i wskazań dla dalszych badań, praktyki czy podejmowania decyzji.

Synteza wykorzystana zostanie podczas opracowywania wszystkich rozdziałów dysertacji. Zgromadzone i przeanalizowane dane zostaną objęte syntezą - szczególnie doty-

[15] J. Apanowicz, *Metodologia nauk,* Wyd. Dom Organizatora, Toruń 2003, s. 26-27.
[16] M. Pelc, *Elementy*…, op. cit*.,* s. 68.

czyć to będzie wyników przeprowadzonych analiz ilościowych. Synteza zostanie zastosowana do opracowania wyników z badań teoretycznych i empirycznych. Pozwoliła ona sformułować problemy badawcze i hipotezy robocze.

Abstrahowanie jest jednym z kluczowych elementów metody naukowej. Polega na wyodrębnianiu istotnych cech, wzorców, zależności lub konceptów z obiektów badawczych i koncentrowaniu się na nich, pomijając mniej istotne szczegóły. Jest to proces umożliwiający skoncentrowanie się na najważniejszych elementach i konceptach, które mają kluczowe znaczenie dla badania lub rozumienia danego obszaru.
Metoda abstrahowania polega na identyfikowaniu ogólnych wzorców, reguł, prawidłowości lub teorii na podstawie obserwacji, analizy danych lub eksperymentów. W ramach tego procesu, badacz dokonuje selekcji i hierarchizacji informacji, aby skupić się na najważniejszych elementach, które mogą mieć największe znaczenie dla dalszych badań, wniosków lub zastosowań praktycznych.

Abstrahowanie umożliwia uproszczenie złożonych rzeczywistości i skupienie się na istotnych aspektach, co ułatwia analizę i zrozumienie badanego zjawiska. Proces abstrahowania może mieć różne formy i metody, w zależności od konkretnej dziedziny nauki i badanego problemu. Polega na zastosowaniu podstawowych operacji myślowych prowadząc do pomijania pewnych składników, cech lub relacji danego układu (przedmiotu, stanu rzeczy), a wyodrębnianiu innych, uznanych za istotne. Jako metoda badawcza może sprowadzać się do czynności: pomijania (eliminowania), odłączania (izolacja) i wyodrębniania. W ramach tej metody, badacz w swoich rozważaniach, powinien uwzględnić elementy, które pod pewnymi względami są nieistotne.[17]

Abstrahowanie jest ważne, ponieważ umożliwia redukcję złożoności i ułatwia koncentrację na istotnych aspektach badanego zagadnienia. Przez abstrahowanie badacze mogą opracować ogólne modele, teorie czy prawa, które mają zastosowanie w szerokim kontekście, a także mogą służyć jako podstawa do dalszych badań, przewidywań czy rozwoju praktyki w danej dziedzinie nauki.

Porównanie to metoda badawczą, która polega na zestawieniu wszystkich cech wspólnych i różnicujących dany przedmiot badań lub zjawisko. Porównanie jest jedną z metod badawczych wykorzystywanych w naukach społecznych oraz innych dziedzinach nauki. Polega na analizie podobieństw i różnic między dwoma lub więcej elementami, by zrozumieć ich charakterystyki, wzorce czy relacje. Metoda porównania może być stosowa-

[17] E. S. Wiśniewski, *Metodyka wojskowych badań naukowych,* Wyd. ASG WP, Warszawa 1990, s. 74.

na na różnych poziomach badania, od analizy indywidualnych przypadków do porównań grupowych, kulturowych czy historycznych.

Autor niniejszej dysertacji przedmiotową metodę badawczą na wszystkich etapach prac badawczych. Jej istotą będzie identyfikacja cech wspólnych oraz podobieństw, ale także różnic poszczególnych zagadnień badawczych, zwłaszcza w zakresie obiegu informacji w organizacji publicznej oraz bezpieczeństwa tego procesu. Porównanie będzie przeprowadzone podczas zestawienia skonstruowanego modelu systemu obiegu informacji w organizacji publicznej z rzeczywistym, obecnie funkcjonującym systemem obiegu informacji.

Wnioskowanie jest kluczową metodą badawczą, która polega na wyciąganiu wniosków, dedukcji lub indukcji na podstawie dostępnych informacji, danych, dowodów lub teorii. Jest to proces logicznego rozumowania, który prowadzi do formułowania nowych informacji, przekonań lub wniosków na podstawie istniejących danych. Rozumowanie polegające na wyprowadzeniu wniosków ze zdań uznanych za prawdziwe, stanowi integralny element procesu badawczego i zostało wykorzystane w niniejszej dysertacji w odniesieniu do całej procedury badawczej. Wnioskowanie zostanie wykorzystane we wszystkich rozdziałach, w części poświęconej wnioskom oraz w zakończeniu rozprawy.

Wnioskowanie jest fundamentalną metodą badawczą, która pomaga w rozumieniu, wyjaśnianiu i generowaniu nowej wiedzy. Poprzez logiczne rozumowanie i wnioskowanie, badacze mogą poszerzać swoją wiedzę, formułować teorie, tworzyć modele oraz wnosić wkład w rozwój nauki w różnych dziedzinach.

Kolejno do metod wnioskowania, zalicza się redukcję i dedukcję.

Redukcja – odnosi się do podejścia badawczego, które polega na analizie i wyjaśnianiu złożonych zjawisk, systemów lub teorii poprzez redukcję ich do prostszych, bardziej podstawowych elementów lub mechanizmów. Redukcja jest stosowana w celu zrozumienia i wyjaśnienia bardziej złożonych aspektów badanego obszaru. O wnioskowaniu na podstawie tej konkretnej metody badawczej możemy mówić wówczas, gdy z przesłanek tego wnioskowania nie wynika jego wniosek, natomiast z wniosku tego wnioskowania wynikają przesłanki[18]. Redukcja może być traktowana jako powrót do następstw przyczyn, pamiętając, że jest to typ wnioskowania zawodnego[19].

[18] K. Ajdukiewicz, *Zarys logiki,* Wyd. PZWS, Warszawa 1956, s. 162.; K. Ajdukiewicz, *Logika pragmatyczna, op. cit.*, s. 127-133.
[19] M. Pelc, *Wybrane problemy metodologiczne wojskowych badań naukowych,* Wyd. AON, Warszawa 1998, s. 18-19.; M. Pelc, *Elementy badań …,* op. cit*.,* s. 24.

Redukcja jest używana w celu uproszczenia i zrozumienia złożonych zjawisk poprzez analizę ich podstawowych składników, mechanizmów lub przyczynowości. Jest to ważne narzędzie w nauce, ponieważ umożliwia badaczom dokładne badanie elementów składowych i procesów, co może prowadzić do lepszego zrozumienia i wyjaśnienia całościowych zjawisk. W badaniu redukcja zostanie zastosowana podczas wskazania, opisania rezultatów stosowania modelu systemu obiegu informacji w organizacji publicznej.

Indukcja – jest to metoda badawcza, która pozwala do wnioskowania ogólnego z przesłanek, wśród których znajdują się zdania jednostkowe stwierdzające poszczególne przypadki ogólnego wniosku. Jest jednym z kluczowych sposobów wnioskowania i generowania wiedzy w naukach empirycznych. Indukcja polega na wyciąganiu ogólnych prawidłowości, reguł lub teorii na podstawie szczegółowych obserwacji, danych lub dowodów. Jest to proces, w którym wnioski są formułowane na podstawie powtarzających się wzorców lub zależności obserwowanych w konkretnych przypadkach.

W oparciu o kanony J. S. Milla zastosowane zostanie podsumowanie indukcji eliminacyjnej, gdzie z jednostkowych zdarzeń wyprowadza się uogólnienie stwierdzające związki przyczynowe. Polega to na tym, iż wnioskuje się, co jest przyczyną bądź składnikiem przyczyny konkretnego zjawiska. Pozwala badaczom generalizować zależności czy reguły na podstawie obserwacji i danych, co prowadzi do rozwijania teorii, tworzenia modeli i zgłaszania hipotez badawczych. Jednak indukcyjne wnioskowanie jest podatne na błędy i ograniczenia, takie jak problem indukcji, czyli niemożliwość pewnego wnioskowania ogólnego na podstawie skończonej liczby obserwacji. Dlatego konieczne jest stosowanie dalszych metod i technik, takich jak dedukcja, eksperymentacja czy weryfikacja, aby potwierdzić i ugruntować wnioski indukcyjne.

Zastosowanie tej metody pozwoli na sformułowanie celów badawczych oraz stworzenie hipotez roboczych.

Dedukcja polega na wyciąganiu wniosków logicznych i nieuniknionych na podstawie pewnych założeń, reguł logicznych i wcześniejszych faktów. Jest to proces, w którym wnioski są wyprowadzane z ogólnych zasad do bardziej szczegółowych sytuacji. To metoda rozumowania polegająca na wyprowadzaniu logicznych wniosków z założeń uznanych za prawdziwe. To rozumowanie polegające na odtwarzaniu faktów (*implicite* i *explicite*) zawartych we wniosku ogólnym[20]. Dedukcją jest nazywane rozumowanie opar-

[20] M. Łobocki, *Wprowadzenie do metodologii badań pedagogicznych*, Wyd. Oficyna Wydawnicza „Impuls", Kraków 2001, s. 50.

te o wnioskowanie formalnie poprawne, czyli realizowane poprzez dany schemat logiczny, np. transpozycję[21].

Dedukcyjne wnioskowanie pozwala na logiczne i niezaprzeczalne rozumowanie na podstawie dostępnych informacji i reguł, co umożliwia rozwijanie teorii i generowanie nowej wiedzy. Dedukcja zostanie zastosowana przy wskazaniu czynników, które mogą wpłynąć na bezpieczeństwo systemu obiegu informacji w organizacji publicznej.

Analogia jest rodzajem wnioskowania, gdyż funkcjonuje w grupie wnioskowania uprawdopodobniającego[22]. Jest to wnioskowanie o posiadaniu pewnej cechy przez dany przedmiot na podstawie jego podobieństwa do innych przedmiotów mających tę właśnie cechę. Jest to metoda stosowana podczas wskazywania podobieństw danych zjawisk i cech.

Analogia jest szczególnie przydatna, gdy badane zjawisko jest trudne do bezpośredniego obserwowania lub badania, a istnieje podobieństwo do innych znanych przypadków. Analogi mogą dostarczać wglądu, sugestii i inspiracji do dalszych badań oraz przyczynić się do rozwijania teorii i generowania nowych hipotez. Jednak należy zachować ostrożność przy stosowaniu analogii, ponieważ nie zawsze podobieństwa gwarantują odpowiednie wnioski, a różnice między przypadkami mogą wprowadzać błędne interpretacje. Jej zastosowanie podczas opracowywania dysertacji pozwala przenosić zależności na inne cechy, czy zjawiska posiadające podobne składowe. Metoda ta będzie zastosowana między innymi przy formułowaniu wniosków o występujących podobieństwach, głównie podczas badania procesów systemu obiegu informacji w organizacjach publicznych.

Uogólnienie ta metoda badawcza odnosi się do procesu wnioskowania, w którym opierając się na ograniczonym zbiorze danych lub przypadków, formułowane są ogólne reguły, zasady lub wzorce dotyczące szerszej populacji lub zjawiska. Uogólnienie jest używane w badaniach naukowych w celu wyciągania wniosków na temat całej populacji lub szerszego zakresu zjawisk na podstawie analizy próby lub podzbioru danych. Polega na rozszerzaniu na ogół lub na duży zakres zjawisk czy faktów twierdzenia - wnioski wyciągnięte z poszczególnych faktów, przesłanek. Jako metoda badawcza jest stosowana w celu ujawnienia cech, powiązań i zależności powtarzalnych, łączenia ich stosowanie do przyjętych kryteriów oraz formułowania na ich podstawie uniwersalnych założeń do koncepcji.

Ważne jest, aby zachować ostrożność i uwzględnić ograniczenia uogólnienia. Ze względu

[21] K. Ajdukiewicz, *Zarys logiki…,* op. cit*.,* s. 160-161.
[22] Z. Ziembiński, *Logika pragmatyczna*, Wyd. Naukowe PWN, Warszawa 2013, s. 191.

na to, że uogólnienie opiera się na analizie ograniczonej próby lub danych, istnieje ryzyko, że wnioski mogą nie odzwierciedlać pełnego obrazu całej populacji lub szerszego zjawiska. Dlatego konieczne jest dbałość o dobranie odpowiedniej próby i przestrzeganie zasad statystyki, aby móc wiarygodnie uogólniać wyniki badawcze. Mimo tych ograniczeń, metoda badawcza uogólnienie jest ważnym narzędziem w naukach społecznych, pozwalając na wnioskowanie na temat większych populacji lub szerszych zjawisk na podstawie ograniczonej próby lub danych.

Uogólnienie będzie zastosowane jako element podsumowujący każdą fazę pracy badawczej oraz w rozdziale końcowym dysertacji, łącząc wyniki badań ilościowych i jakościowych.

Jak już wspomniano powyżej w pracy oprócz metod teoretycznych zastosowane zostaną także metody empiryczne. Będą to metody obserwacji oraz badania opinii, które są charakterystyczne dla badań naukowych prowadzonych w naukach społecznych. Podczas empirycznych badań autor będzie starał się głównie poznać sądy, opinie, motywy, procedury i procesy wykonawcze, ale także oczekiwania przez badanych. Obserwacja zachowań badanych, doprowadzi do nagromadzenia i stworzenia zasobu nowych faktów naukowych.

Przyjmuje się, że zamierzeniem badań empirycznych jest poznanie określonych zjawisk społecznych poprzez bezpośredni kontakt podmiotu i przedmiotu badań[23]. Realizacja tego postulatu odbędzie się za pośrednictwem obserwacji, którą można zdefiniować jako ukierunkowane, zamierzone oraz systematyczne postrzeganie badanego przedmiotu, procesu lub zjawiska[24]. To uważne przyglądanie się czemuś lub komuś przez dłuższy czas, czego efektem są wynik takiego obserwowania. Metoda naukowa obserwacja jest jednym z podstawowych narzędzi badawczych w naukach empirycznych. Obserwacja polega na systematycznym i świadomym zbieraniu informacji na temat zjawisk, obiektów, zachowań lub procesów, które można bezpośrednio zaobserwować zmysłami lub za pomocą odpowiednich narzędzi pomiarowych. Jest wykorzystywana zarówno w badaniach jakościowych, jak i ilościowych. Obserwacja może dostarczać wglądu w rzeczywiste zachowanie, procesy czy interakcje, a także stanowi podstawę dla dalszych analiz, wnioskowań i teorii. Jednak obserwacja może być również podatna na błędy, subiektywność interpretacji czy ograniczenia związane z warunkami obserwacji. Dlatego ważne jest, aby obserwacja była

[23] B. Szulc, *Proces badań w naukach o obronności*, Praca naukowo-badawcza, Kod pracy: II.2.24.2., AON, Warszawa 2014, s. 68.
[24] J. Sztumski, *Wstęp do metod…*, *op. cit.,* s. 112.; J. Pieter, *Ogólna metodologia…,* op. cit., s. 108-112.

przeprowadzana w sposób kontrolowany i uwzględniała restrykcyjne metody badań naukowych.

Opisywana metoda badawcza wykorzystana będzie podczas analizy realizacji procesów obiegu informacji w organizacji publicznej.

Zastosowanie metody obserwacji, rozumianej jako czynności badawczej polegającej na gromadzeniu danych drogą postrzeżeń[25], nie będzie miała na celu falsyfikowania czy weryfikowania konkretnej teorii (hipotezy), ale da możliwość poznania rzeczywistości będącej przedmiotem badań. Obserwacja użyta zostanie zgodnie z definicją podaną przez T. Kotarbińskiego - jako sposób wykonywania czynu złożonego polegającego na określonym doborze i układzie jego działań składowych, a przy tym uplanowany i nadający się wielokrotnego stosowania[26].

W procesie obserwacji naukowej istnieje kilka kluczowych aspektów:

1. Cel obserwacji: Przed przystąpieniem do obserwacji naukowej, badacz musi określić jasno cel badania. Cel może obejmować zrozumienie danego zjawiska, identyfikację wzorców, badanie relacji przyczynowo-skutkowych, weryfikację teorii lub testowanie hipotez.
2. Plan obserwacji: Badacz opracowuje plan obserwacji, który obejmuje wybór odpowiednich technik obserwacyjnych, określenie kryteriów obserwacji, identyfikację kontekstu i warunków obserwacji oraz ustalenie jednoznacznych definicji i kategorii obserwowanych zjawisk.
3. Rejestrowanie danych: Podczas obserwacji badacz rejestruje systematycznie dane na podstawie obserwacji. Mogą to być dane jakościowe, takie jak opisy zachowań, reakcje, interakcje, obserwacje środowiska, jak również dane ilościowe, takie jak pomiary czasu, odległości, ilości itp.
4. Uważność i dokładność: Ważne jest, aby badacz był uważny, skoncentrowany i dokładny podczas obserwacji, aby nie przeoczyć istotnych informacji. Powtarzalność obserwacji przez różnych badaczy może również pomóc w potwierdzeniu spójności wyników.
5. Analiza danych: Zebrane dane są analizowane w celu zrozumienia, klasyfikowania, porządkowania lub opisywania obserwowanych zjawisk. Analiza może obejmować wykorzystanie statystyki, technik kodowania, kategoryzacji lub tworzenie wzorców i tema-

[25] T. Pilch, T. Bauman, *Zasady badań pedagogicznych*, Wyd. Zakład Narodowy im. Ossolińskich, Wrocław-Warszawa-Kraków-Gdańsk 1977, s. 128.
[26] T. Kotarbiński, *Traktat o dobrej robocie,* Wyd. Zakład im. Ossolińskich, Wrocław 1955, s. 88.

tów.

W odniesieniu do analizy procesów systemu obiegu informacji w organizacji publicznej, przedmiotem badań będzie rzeczywista realizacja tych procesów. Wieloaspektowość przedmiotu badań stanie się przyczynkiem do stworzenia narzędzia badawczego mającego charakter porządkujący obserwowane elementy w następujących obszarów:

- cel sytemu obiegu;
- role/osoby wykonujące czynności w systemie obiegu;
- podejmowane decyzje w systemie obiegu;
- etap systemu obiegu;
- rozpoczęcie/zakończenie obiegu;
- (ewentualne) elementy optymalizacji systemu obiegu.

W metodzie tej można gromadzić materiały w sposób nieszablonowy poprzez swobodne notatki, opisy, fotografie, nagrania lub szablonowy, wykorzystując arkusz obserwacji lub dziennik obserwacji.

W celu utrwalenia jak największej liczby spostrzeżeń zostanie skonstruowany Arkusz obserwacji, który posłuży podczas procesu badawczego jako rzetelne narzędzie do obserwacji procesów obiegu informacji w organizacji publicznej. Obserwator, w tym przypadku autor dysertacji, podczas procesu obserwacji postara się być spostrzegawczy, przy zachowaniu rzetelności, obiektywności, wnikliwości i wyczerpująco notować swoje spostrzeżenia.

Główną cechą metody obserwacji jest jej bezpośredniość. Podczas stosowania metody obserwacji zbierana są dane bezpośrednie, przez co unika się oddziaływania czynników stojących pomiędzy badaczem, a przedmiotem badań. Dane, które są zbierane podczas obserwacji są odzwierciedleniem tego, w jaki sposób dane zjawisko przebiega w naturalnych warunkach. Kolejnym aspektem obserwacji jest to, że osoba badana w wielu przypadkach nie jest świadoma procesu obserwacji przebiegającego wokół niej. Częstym zjawiskiem jest to, że osoba badana szybko się przyzwyczaja do obserwatora i nie traktuje obserwatora jako wroga czy intruza[27].

Ze względu na charakter prowadzonych badaniach zostaną wykorzystane wszystkie formy obserwacji wyróżnione w literaturze:

- indywidualna i zbiorowa;
- bierna lub uczestnicząca;

[27] D. Nachmias C. Frankfort-Nachmias, *Metody badawcze*…, op. cit., s. 223-224.

- bezpośrednia lub pośrednia;
- ciągła lub okresowa[28];

Dodatkowo obserwacja będzie wykorzystana jako technika w procesie działalności badawczej. W początkowej fazie badań obserwacja przyczyni się do refleksji nad sytuacją problemową, będącą wyjściem do podjętych badań i sformułowania celu ich prowadzenia.

Autor dysertacji zakłada, że główną rolę podczas procesu badawczego będzie pełnić metoda wywiadu sondażu diagnostycznego. Będzie ona przyczynkiem do rozwiązania większości szczegółowych problemów badawczych, których wyniki zostaną zaprezentowane w całości w rozdziale czwartym. Zastosowanie tej metody badawczej wynika z przedmiotu i celu badań. Metoda ta polega na statystycznym sposobie zbierania informacji o faktach, zjawiskach i procesach oraz o dynamice ich rozwoju.

Metoda naukowa sondaż diagnostyczny odnosi się do techniki badawczej, która ma na celu diagnozowanie, identyfikowanie i analizowanie określonych cech, problemów lub stanów w populacji lub badanej grupie. Sondaż diagnostyczny jest stosowany w różnych dziedzinach, takich jak psychologia, socjologia, medycyna czy edukacja, aby zdobyć informacje diagnostyczne i lepiej zrozumieć badane zagadnienia. Sondaż diagnostyczny ma na celu dostarczenie informacji diagnostycznych, które mogą być wykorzystane do lepszego zrozumienia badanych.

Proces sondażu diagnostycznego obejmuje kilka kluczowych etapów:

1. Określenie celu: Badacz określa jasno zdefiniowany cel sondażu diagnostycznego, czyli problem, cechę lub stan, który ma być diagnozowany.
2. Projektowanie sondy: Badacz projektuje narzędzia i metody sondażu diagnostycznego, które będą używane do zebrania danych. Narzędzia mogą obejmować kwestionariusze, skale ocen, testy, obserwacje lub wywiady. Ważne jest, aby narzędzia były odpowiednio dostosowane do celu sondażu diagnostycznego i miały wysoką jakość psychometryczną.
3. Wybór próby: Badacz wybiera reprezentatywną próbę, czyli grupę osób lub obiektów, która ma być badana w sondażu diagnostycznym. Ważne jest, aby próba była reprezentatywna dla całej populacji lub badanej grupy, aby wyniki były generalizowalne.
4. Zbieranie danych: Badacz zbiera dane za pomocą wybranych narzędzi i metod sondażowych. Może to obejmować przeprowadzanie ankiet, przeprowadzanie wywiadów, przeprowadzanie obserwacji lub przeprowadzanie testów. Dane są zbierane w sposób

[28] J. Apanowicz, *Metodologia ogólna*…, op.cit., s. 84.

systematyczny i starannie dokumentowane.

5. Analiza i interpretacja danych: Zebrane dane są analizowane w celu oceny i interpretacji badanych cech, problemów lub stanów. Analiza danych może obejmować statystyczne metody, porównania grupowe, identyfikację wzorców czy tworzenie profilów diagnostycznych.
6. Wnioski i zalecenia: Na podstawie analizy danych badacz wyciąga wnioski dotyczące diagnozowanych cech, problemów lub stanów. Wnioski mogą prowadzić do dalszych działań, takich jak opracowanie interwencji, formułowanie zaleceń terapeutycznych lub wprowadzenie zmian w praktyce.

Realizacja badań z wykorzystaniem metody sondażu diagnostycznego będzie prowadzona przy użyciu techniki ankiety. Zostanie zastosowana technika ankiety audytoryjnej, przy użyciu narzędzia badawczego, jakim jest kwestionariusz ankiety. Zastosowane narzędzie pozwoli zdobyć obszerny materiał empiryczny z zakresu omówionego problemu badawczego. Ma ona charakter anonimowy, a zatem pozwala na uzyskanie od respondentów szczerych, zgodnych z ich przekonaniami odpowiedzi.

Kwestionariusz ankiety zostanie opracowany jako narzędzie standaryzowane częściowo ustrukturalizowane. Wszyscy respondenci posługiwać się będą takim samym zestawem pytań przedstawionych w stałej kolejności, a pytania będą skonstruowane z jednoznacznej kafeterii odpowiedzi.

Wykonane badania empiryczne przeprowadzone zostały w celu zbadania opinii funkcjonariuszy Państwowej Straży Pożarnej. Założono, iż wszyscy strażacy realizują swoje zadania uczestnicząc w systemie obiegu informacji PSP. Kolejno przyjęto założenie, ze w Polsce zatrudnionych jest ok. 30000 tysięcy zawodowych funkcjonariuszy PSP i pracowników korpusu służby cywilnej, z czego ok. 28000 tyś. pracuje w Komendach Powiatowych/Miejskich, natomiast ok. 2000 w Komendach Wojewódzkich. Z uwagi na powyższe założenie dokonano doboru próby badawczej wynikające z potrzeby przeprowadzenia badań za pomocą kwestionariusza ankiety i sposobu doboru losowego prostego zależnego[29], który polega na nieograniczonym i bezpośrednim doborze potencjalnych jednostek badania do próby statystycznej. W owym sposobie nie jest możliwe zwracanie wylosowanej jednostki z powrotem do populacji. Umożliwiło to bowiem jednokrotne uczestnictwo poszczególnych jednostek. Wyznaczenie próby badawczej ukierunkowane było nie

[29] M. Cieślarczyk (red. nauk.), *Metody, techniki i narzędzia badawcze oraz elementy statystyki stosowane w pracach magisterskich i doktorskich*, Wydawnictwo AON, Warszawa 2006 r., s. 47.

tylko wielkością badanej populacji, ale również chęcią i dążeniem do uzyskania precyzyjnych jak i wiarygodnych wyników.

Zasadniczym jednak było przeprowadzenie odpowiednich obliczeń, które umożliwiły określenie niezbędnej wielkości próby badawczej, a mianowicie:

$$n_b = \frac{N}{1 + \frac{d^2\,(N-1)}{z^2\,pq}}$$

Gdzie:

N – liczebność próby;

z – parametr poziomu ufności, z = 1,96 przy α = 0,05;

p – spodziewany rząd wielkości szacowanej frakcji;

q – 1-p;

d – dopuszczalny błąd pomiaru.

Przyjęto, iż parametr ufności (z) w naukach społecznych jest stały i wynosi 1.96, przy poziomie ufności (p) równym 0,5. Błąd pomiaru analogicznie przyjęto jako wielkość statystycznie stałą, wyrażoną w setnych jako (D= 0,05). Przyjęto, iż wartość wskaźnika N dla Komend Wojewódzkich PSP wynosi 1 960 (co stanowi 98% z 2000 osób), a dla Komend Miejskich/Powiatowych PSP - 27 440 (co stanowi 98% z 28000). W świetle powyższego, obliczono dwie wielkości próby. Dla KW PSP minimalna wielkość próby ukształtowała się na poziomie 321 osób, a dla KM/KP PSP 379 osób.

$$n_{b\ KW+KG} = \frac{1960}{1+\frac{0{,}05^2\,(1960-1)}{1{,}96^2\ x\ 0{,}5\,(1-0{,}5)}} = 321$$

$$n_{b\ KM/KP} = \frac{27440}{1+\frac{0{,}05^2\,(27440-1)}{1{,}96^2\ x\ 0{,}5\,(1-0{,}5)}} = 379$$

Badania zostały ukończone w styczniu 2023 roku. W wyniku przeprowadzonych badań w obu grupach uzyskano łącznie 1897 poprawnie uzupełnionych kwestionariuszy ankietowych, z czego 352 dla Komend Wojewódzkich i Komendy Głównej PSP oraz 1545 dla Komend Miejskich/Powiatowych PSP.

Respondentów scharakteryzowano na podstawie czterech kryteriów:

- wieku badanych,
- doświadczenia (stażu służby),
- struktury wykształcenia,
- zajmowanego stanowiska (dowódcze, wykonawcze).

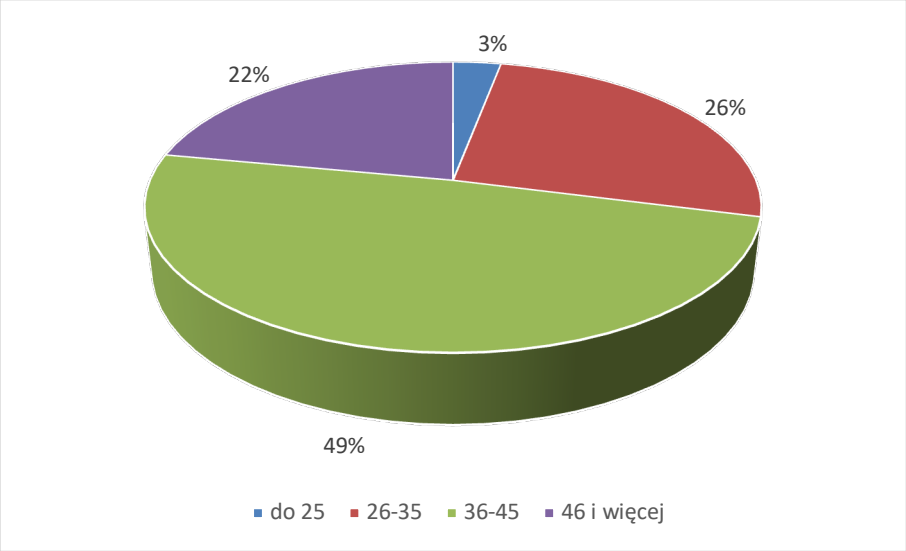
Tabela 1-1
Charakterystyka ankietowanych pod względem wieku.

Wiek	Liczba wskazań	Procent [%]
do 25	64	3
26-35 lat	491	26
36-45 lat	935	49
46 lat i więcej	407	22
SUMA	**1897**	**100**

Źródło: opracowanie własne

W badaniach empirycznych wzięło udział 1897 ankietowanych osób, z których tylko 3 % było wieku poniżej 25 lat, 26 % w wieku 26-35 lat, 49 % w wieku 36-45 lat oraz 22 % powyżej 46-tego roku życia.

Wykres 1-1
Charakterystyka ankietowanych pod względem wieku.



Źródło: *opracowanie własne*

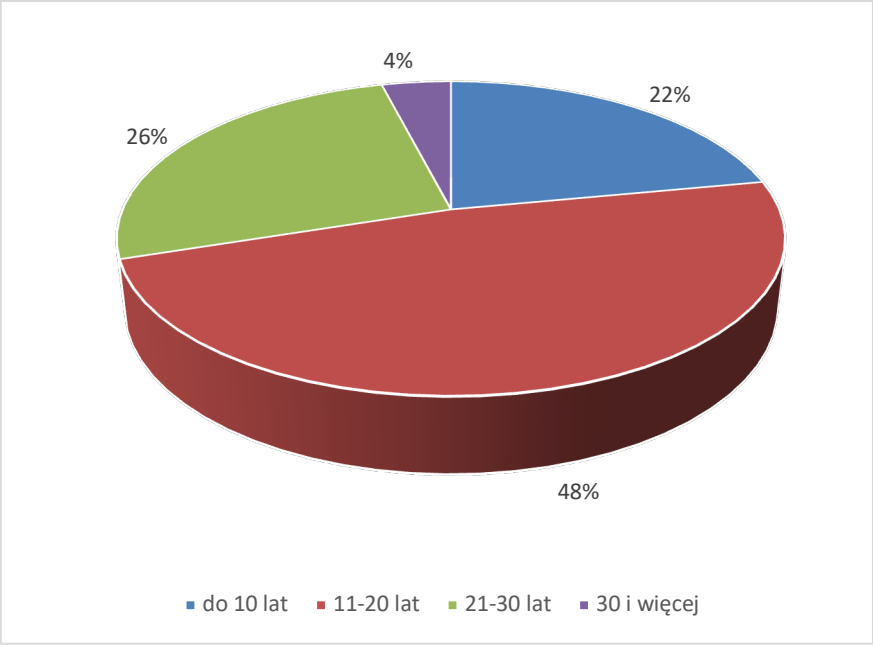
Tabela 1-2
Charakterystyka ankietowanych pod względem stażu zawodowego.

Staż	Liczba wskazań	Procent [%]
do 10 lat	424	22
11-20 lat	920	48
21-30 lat	501	26
31 i więcej	52	4
SUMA	**1897**	**100**

Źródło: *opracowanie własne*

W odniesieniu do kryterium doświadczenia zawodowego do przedziału do 10 lat stażu należało – 424 wskazania (22 %), potem 11-20 lat – 920 wskazań (48 %), następnie, 21 – 30 lat 501 wskazań (26 %) i 31 lat i więcej522 wskazania (4 %).

Wykres 1-2
Charakterystyka ankietowanych pod względem stażu zawodowego.



Źródło: *opracowanie własne*

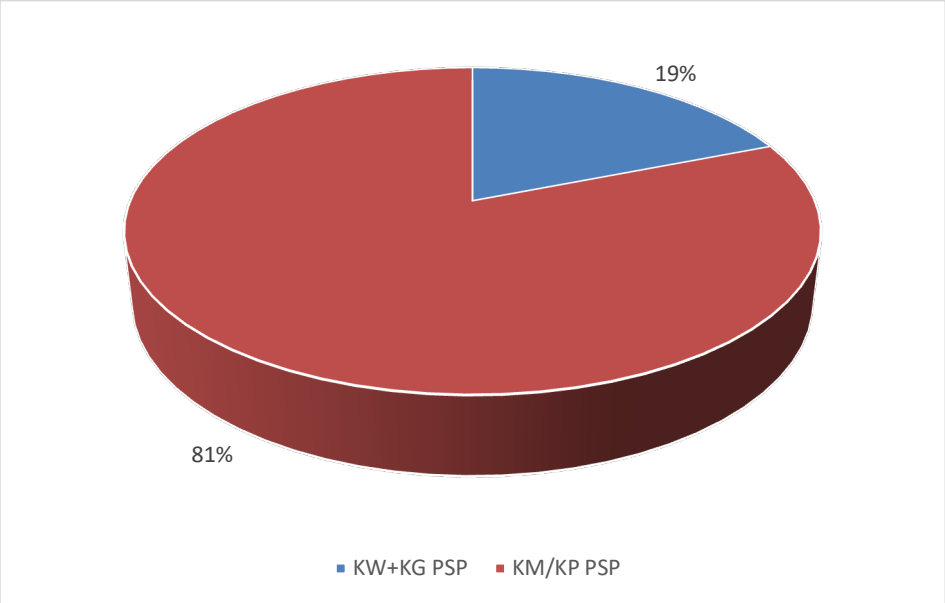
Tabela 1-3
Charakterystyka ankietowanych według kryterium miejsca zatrudnienia.

Miejsce zatrud-nienia	Liczba wskazań	Procent [%]
KW PSP	352	19
KM/KP PSP	1545	81
SUMA	**1897**	**100**

Źródło: *opracowanie własne*

Według kryterium zatrudnienia respondentów 81 % (1545 wskazań) badanej populacji było zatrudnionych w Komendach Miejskich i Powiatowych Państwowej Straży Pożarnej, natomiast 19 % (352 wskazań) stanowiły osoby pracujące w Komendach Wojewódzkich i Komendzie Głównej Państwowej Straży Pożarnej.

Wykres 1-3
Charakterystyka ankietowanych według kryterium zatrudnienia.



Źródło: *opracowanie własne*

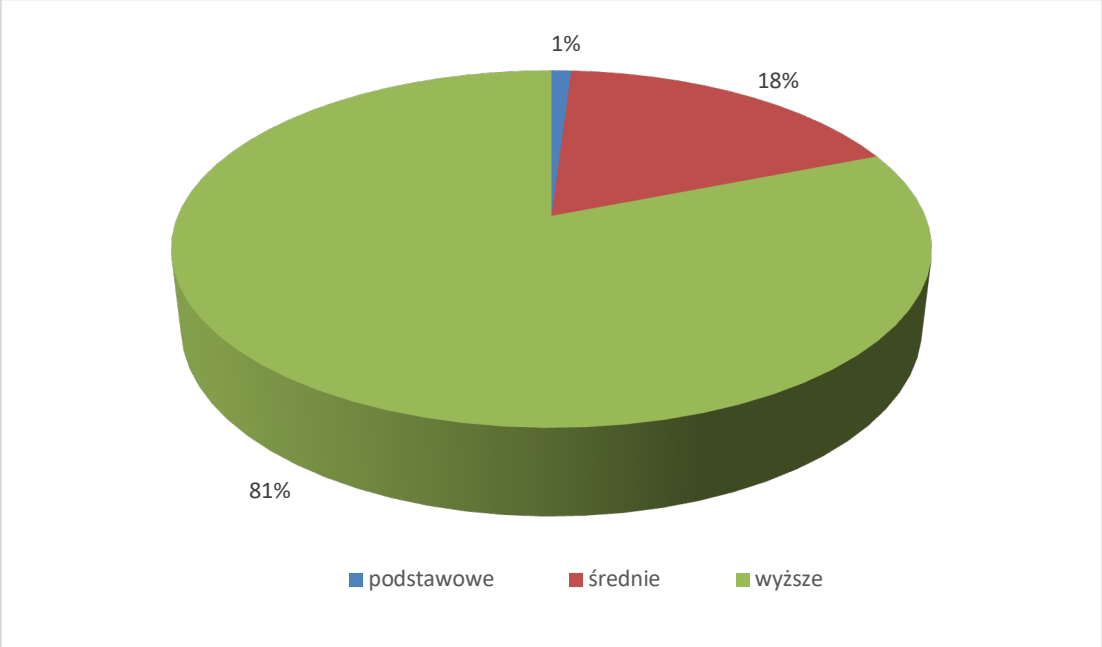
Tabela 1-4
Charakterystyka ankietowanych pod względem wykształcenia.

Wykształcenie	Liczba wskazań	Procent [%]
podstawowe	2	1
średnie	339	18
wyższe	1556	81
SUMA	**1897**	**100**

Źródło: *opracowanie własne*

Analizując ankietowanych pod kątem ich wykształcenia, to najwięcej osób posiadało wykształcenie wyższe 81 % (1556 wskazań). Następnie, średnie 18 % (339 wskazania) dwie osoby z wykształceniem podstawowym, co daje niespełna 1 % ankietowanych.

Wykres 1-4
Charakterystyka ankietowanych pod względem wykształcenia.



Źródło: *opracowanie własne*

W celu określenia siły związku pomiędzy zmiennymi – odpowiedziami respondentów należących do różnych grup statystycznych - wykorzystano elementy statystyki. Obliczenia te były szczególnie przydatne do ustalenia związku sądów oraz opinii z przynależnością do poszczególnych grup respondentów oraz do syntezy myślowej cząstkowych opinii i sądów uzyskanych w trakcie badań ankietowych w celu uogólnienia uzyskanych wyników. W tym przypadku posłużono się współczynnikiem korelacji r Pearsona, który służy do sprawdzenia czy dwie zmienne ilościowe są powiązane ze sobą związkiem liniowym.

Jednak w związku z tym, że badania przeprowadzone były na próbie badawczej, obliczony współczynnik siły związku (korelacji) upoważniał jedynie do formułowania tylko prawdopodobnych wniosków o określonej sile współzależności między zmiennymi.

W celu zbadania istotności współzależności wyników (siły związku między przynależnością do danej grupy respondentów, a siłą sądów na badane zagadnienie) wykonano test współczynnika korelacji liniowej r – Pearsona, zgodnie ze wzorem.

$$r = \frac{\frac{1}{n}\sum_{i=n}^{n} x_i y_i - \bar{x}\bar{y}}{\sqrt{(\frac{1}{n}\sum_{i=n}^{n} x_i^2 - \bar{x}^{2)})\,(\frac{1}{n}\sum_{i=n}^{n} y_i^2 - \bar{y}^{2)})}}$$

Gdzie:

- $xiyi$ - wartości obserwacji z populacji X i Y;
- $\bar{x}$, $\bar{y}$ - średnie z populacji X i Y;
- σx, σy - odchylenie standardowe populacji X i Y;
- n - ilość obserwacji (X jak i Y mają po tyle samo obserwacji).

Podobnie jak inne współczynniki korelacji również wynik r Pearsona może wahać się od -1 do 1. Wartości skrajne, czyli -1 i 1 oznaczają idealną, totalną korelację między zmienną A i zmienną B. Wynik równy "zero" oznacza brak współwystępowania wartości tych dwóch zmiennych w naturze (brak korelacji).

Interpretacja współczynnika korelacji r Pearsona w naukach społecznych przebiega w następujący sposób:

W ramach interpretacji korelacji można wyróżnić następujące rodzaje korelacji:

- dodatnia,
- ujemna,

• brak korelacji.

Wartości r:

< 0,3	korelacja słaba
0,4-0,6	korelacja umiarkowana
0,7-0,9	korelacja silna
1	korelacja idealna

Korelacja dodatnia, czyli r > 0 tyczy się kiedy wartość X rośnie i jednocześnie z nią rośnie wartość Y. Dodatnia korelacja pojawia się wówczas, kiedy wzrostowi cech jednej wartości towarzyszy wzrost drugiej cechy.

Korelacja ujemna, czyli r < 0 tyczy się kiedy X rośnie, a Y maleje. Korelacja ujemna ma miejsce wówczas, gdy wzrostowi wartości jednej cech towarzyszy spadek optymalnych wartości drugiej cechy.

Brak korelacji r = 0 występuje, kiedy X rośnie, a Y czasami rośnie albo maleje.

Podając za M. Bojańczyk korelacja zachodząca między zmiennymi X i Y jest miarą siły liniowego związku pomiędzy nimi. Ową analizę związku liniowego należy rozpocząć od zaprojektowania wykresu, określanego mianem wykresu rozrzutu punktowego[30].

Podkreślić w tym miejscu należy, że r wyliczane jest tylko wówczas, gdy obie zmienne mają rozkład zbliżony do normalnego i posiadają wartość mierzalną oraz gdy pojawia się zależność prostoliniowa. Uwzględniając powyższe uwarunkowania powstało określenie korelacji liniowej. Odnosząc się do interpretacji współczynnika r, należy mieć na względzie, iż nie zawsze wartość bliska zera oznacza brak zależności, bowiem może wskazywać zaledwie brak zależności liniowej[31].

W przeprowadzonych badaniach, których szczegółowe wyniki zaprezentowane zostaną w rozdziale 4.1 poprzez analizę wyników, wskazano, czy zachodzi związek pomiędzy poszczególnymi zmianami. Sprawdzono czy dane odpowiedzi związane są z przynależnością ankietowanych do przypisanych grup badawczych (KW PSP oraz KM/KP PSP). Badania dokonano na próbie badawczej jednocześnie obliczony współczynnik korelacji, pozwolił sformułować prawdopodobne wnioski o odpowiedniej sile współzależności między zmiennymi.

[30] M. Bojańczyk, *Regresja i korelacja na światowych rynkach- w pułapce metod ilościowych*, „Kwartalnik Naukowy Uczelni Vistula", nr 4, 2013 r., s. 77.

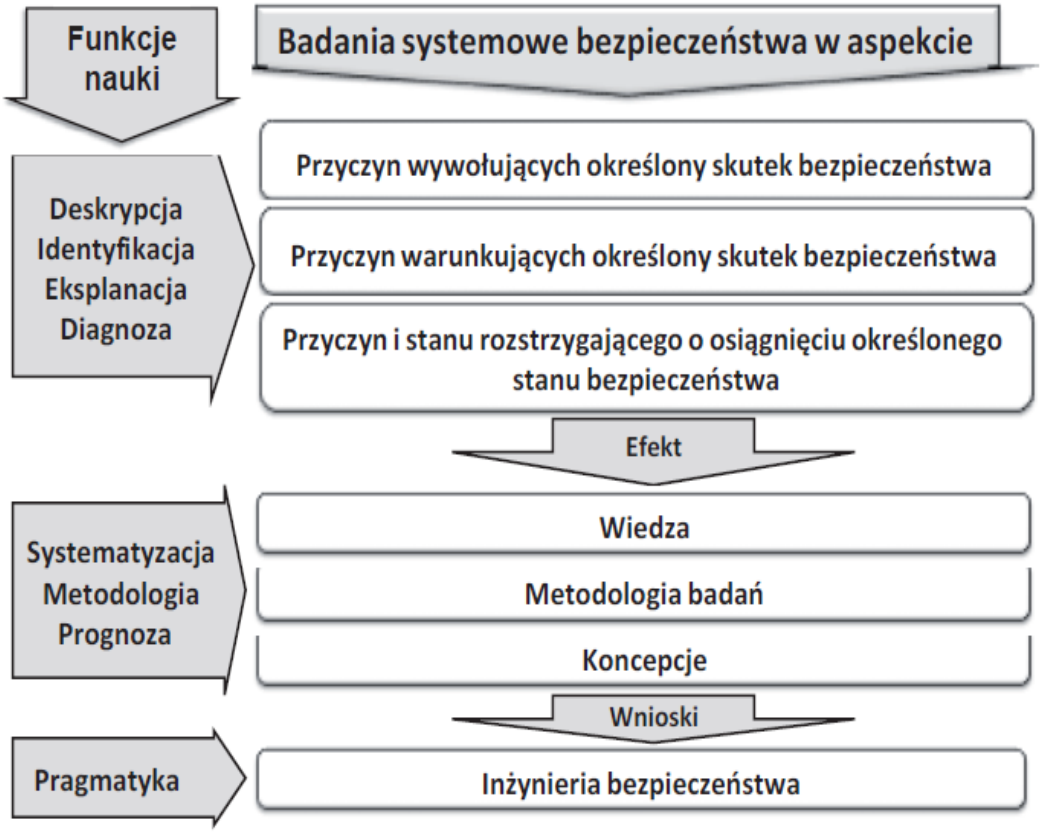
[31] E. Kulawiecka, *Rachunek korelacji w naukach o bezpieczeństwie z wykorzystaniem programu Statistica*, Wyd. Obronność - Zeszyty Naukowe Wydziału Zarządzania i Dowodzenia Akademii Obrony Narodowej, Numer 4(20) (2016) s. 370.

1.6 PROCES BADAŃ

Zgodnie z definicją B. Szulca proces badawczy należy rozumieć jako swoisty układ występujących kolejno czynności realizowanych przez określone podmioty, zmierzających do określonego celu poznawczego[32].

W kontekście prowadzonych rozważań można zatem postawić tezę, że podejście do badań odbędzie się w sposób systemowy, z następującymi założeniami[33]:

- obiekt badań traktowany będzie jako system,
- system postrzegany jest jako podsystem należący do większego systemu,
- w badanym systemie znajdują się inne podsystemy,
- należy stosować racjonalne optymalizowanie systemu.



Źródło: Praca zbiorowa – *„Ochrona przeciwpożarowa a bezpieczeństwo państwa”*, Wyd. CNBOP-PIB, Józefów 2014 r., s. 33

Rysunek 1-4
Badania systemowe bezpieczeństwa w ujęciu nauki.

[32] B. Szulc, *Proces badań ...,* op. cit., s. 56-60.
[33] P. Sienkiewicz, *Podstawy teorii systemów*, Wydawnictwo AON, Warszawa 1993 r., s. 65.

Proces badawczy dla niniejszej dysertacji zostanie zrealizowany w trzech fazach, a uszczegółowienie czynności badawczych zostało zaprezentowane w zamieszczonej poniżej Tabeli 5.

- Faza I – przygotowanie badań;
- Faza II – prowadzenie badań;
- Faza III – opracowanie badań.

Faza pierwsza nazywa się fazą planowania. Obejmie ona określenie podstawowych elementów procesu badawczego poprzez operacjonalizację zmiennych konceptualnych na język doświadczeń. W tej części procesu badawczego dojdzie do wstępnego określenia pomysłu, celu, przedmiotu badań, wstępnych zmiennych oraz sformułowania problemów badawczych i hipotez. Następnie w ramach czynności planistycznych (w ramach fazy przygotowawczej) autor dobierze metody, próbę badawczą, teren badań w celu finalnego skonstruowania narzędzi badawczych. Powyższe działania zostaną zrealizowane w oparciu o wstępną analizę literatury przedmiotu.

Zatem czynności tej fazy można usystematyzować według następującej kolejności:

- pomysł badań;
- określenie celu badań i ustalenie podmiotu;
- wstępne określenie zmiennych;
- konceptualizacja i operacjonalizacja;
- formułowanie problemów badawczych oraz hipotez roboczych;
- dobór metod i technik badawczych;
- dobór próby badawczej oraz określenie terenu badań;
- przygotowanie narzędzi badawczych;

Druga faza, czyli faza badań właściwych, to działalność poznawcza skoncentrowana na zastosowaniu procedur metod teoretycznych lub empirycznych w zależności od charakteru prowadzonych badań (jakościowych i ilościowych).

Etap działalności twórczej badacza to trzeci etap procesu badawczego, jest to właściwe zakończenie badań. Podczas tej fazy zostanie opracowana koncepcja systemu obiegu informacji w organizacji publicznej. W fazie tej opracowane zostały możliwości wprowadzenia usprawnień w bezpieczeństwie systemu informacyjnego Państwowej Straży Pożarnej, poprawiające skuteczność jej funkcjonowania jako organizacji zhierarchizowanej w obszarze organizacyjnym, technicznym i funkcjonalnym. Zanim jednak finalnie to nastąpiło, w pierwszej kolejności doszło do klasyfikowania, kategoryzowania

i selekcjonowania zgromadzonego materiału badawczego, który ostatecznie zostanie poddany wnioskowaniu końcowemu[34]. J. Sztumski dokładnie precyzuje wymagania odnoszące się do analizy zgromadzonych materiałów podczas procesu badawczego. Pierwszym krokiem podczas analizy będzie weryfikacja, która polega na ustaleniu wartości zebranych danych w odniesieniu do zebranych informacji oraz sposobu metodologicznej poprawności ich pozyskania.

Następnie materiały będzie należało poddać selekcji polegającej na eliminacji danych zaburzających metodologiczny rygor badawczy. Dalszym krokiem będzie klasyfikacja, czyli logiczny podział danych zgodnie z przyjętym porządkiem.

Kolejnym krokiem będzie kategoryzacja materiałów polegająca na uporządkowaniu materiałów według potrzeb, zachowując cechę rozłączności kategorii i nawiązywania do celu badań. Ostatnią czynnością będzie skalowanie danych w zależności od potrzeb prowadzonych badań i badacza ich prowadzących. Skalowanie polega na przypisywaniu istotnym dla badania wartościom (wskaźnikom) cech liczbowych lub innych znaków pełniących funkcję narzędzi pomiaru.

Ograniczenia badań jest to element występujący w każdym procesie badawczym. Ograniczenia badań są związane z zastosowanymi metodami i technikami badawczymi.

Poznanie jakościowe jest uwarunkowane słabościami wynikającymi z[35]:

- przypadkowym gromadzeniem danych;
- niesystematyczną analizą danych;
- dowolnym traktowaniem tworzenia teorii;
- problemami wykorzystania danych do testowania teorii;
- niespełnienia kryteriów intersubiektywnej sprawdzalności.

Natomiast, poznanie ilościowe jest obarczone słabościami związanymi z[36]:

- uznaniem deklaracji czy opinii ujętych w ramy pomiaru za rzeczywiste fakty społeczne;
- tendencją do uszczuplania opisu jakościowego zebranych danych ilościowych;
- nieprecyzyjnym, zbyt wąskim określeniem badanego zjawiska;
- pochopnym wyciąganiem wniosków z analizy jakościowej;
- wadliwym opracowaniem narzędzia;

[34] Por.: J. Sztumski, *Wstęp do metod…*, op. cit., s. 156-161.
[35] W. Czakon, *Podstawy metodologii w naukach o zarzadzanie*, Wydawnictwo Oficyna, Warszawa 2013., s.10-111.
[36] M. Łobocki, *Wprowadzenie do metodologii…,* op. cit*.,* s. 80-84.

- problemami ze zrozumieniem instrukcji poprzedzającej badanie, dotyczącej jego istoty czy przedmiotu, co może zaważyć jakościowo na trafności całego badania.

Tabela 1-1
Etapy przeprowadzonego procesu badawczego.

Fazy	Czynności	
Faza 1. Faza przygotowawcza	**Krok 1**	Pomysł badań: • kilkuletnie, osobiste zainteresowanie tematyką oraz doświadczenie związane z systemem obiegu informacji, w tym obiegiem realizowanym w ramach funkcjonowania organizacji publicznych; • analiza obserwacji, doświadczeń i studium przypadków, które zdobyto głównie podczas pracy w ramach obiegu informacji w organizacji publicznej, a to umożliwiło zidentyfikować sytuację problemową.
	Krok 2	Określenie celu i przedmiotu badań.
	Krok 3	Początkowe określenie zmiennych.
	Krok 4	Konceptualizacja ba dań (oparta między innymi na wstępnej analizie literatury przedmiotu): 1. Formułowanie problemów badawczych oraz hipotez roboczych. 2. Dobór metod i technik badawczych. 3. Dobór próby badawczej oraz określenie terenu badań. 4. Opracowanie koncepcji rozprawy doktorskiej.
	Krok 5	Operacjonalizacja oraz przygotowanie narzędzi badawczych.
Faza 2. Faza badań właściwych	**Krok 6**	Analiza krytyczna treści literatury (dokumentów), m.in. pod kątem: • modelu systemu obiegu informacji w organizacji publicznej; • bezpieczeństwa systemu obiegu informacji w organizacji publicznej;
	Krok 7	Dobór próby badawczej.
	Krok 8	Weryfikacja narzędzi badawczych - kwestionariusza ankiety.
	Krok 9	Przeprowadzenie badań empirycznych w kolejności: 1. Badania ankietowe. 2. Opracowanie modelu systemu.

Źródło: opracowanie własne na podstawie: B. Szulc, *Proces badań w naukach o obronności*, *Praca naukowo-badawcza,* Kod pracy: II.2.24.2., Wyd. AON, Warszawa 2014, s. 56-60

Tabela 1-4 cd.
Etapy przeprowadzonego procesu badawczego.

Fazy	Czynności	
Faza 3. Faza opracowania wyników badań	**Krok 10**	Porządkowanie i grupowanie zebranych materiałów badawczych (weryfikacja, selekcja, klasyfikacja, kategoryzacja, skalowanie danych).
	Krok 11	Prezentowanie uzyskanych danych.
	Krok 12	Analiza jakościowa i ilościowa materiału badawczego.
	Krok 13	Interpretacja wyników badań.
	Krok 14	Weryfikacja hipotez.
	Krok 15	Opracowanie koncepcji bezpieczeństwa systemu obiegu informacji w organizacji publicznej.
	Krok 16	Wnioskowanie końcowe.
	Krok 17	Opracowanie pisarskie badań w formie dysertacji.

Źródło: opracowanie własne na podstawie: B. Szulc, *Proces badań w naukach o obronności, Praca naukowo-badawcza*, Kod pracy: II.2.24.2., Wyd. AON, Warszawa 2014, s. 56-60.

Rozdział 2 PODSTAWY ZARĄDZANIA BEZPIECZEŃSTWEM SYSTEMU INFORMACYJNEGO W INSTYTUCJACH PUBLICZNYCH.

Realizacja bardzo dużej liczby zadań i celów postawionych przed jednostkami administracji publicznej państwa, w tym dla Państwowej Straży Pożarnej, bez wątpienia powoduje konieczność wykorzystania coraz to bardziej nowoczesnych technologii. Instytucje realizujące zadania publiczne wykorzystują na co dzień szereg różnych, często skomplikowanych, systemów teleinformatycznych. Proces ten wymaga przetwarzania wielu bardzo różnych i obszernych zbiorów danych. Instytucje rządowe i samorządowe, to podmioty przetwarzające najszerszy z możliwych zakres informacji. Mając na uwadze rosnące znaczenie wykorzystywanych przez te podmioty ilości systemów informacyjnych, niezwykle istotne wydaje się zwrócenie uwagi na systemem zarządzania bezpieczeństwem informacji w tych organizacjach.

W Państwowej Straży Pożarnej przetwarzane są również informacje niejawne oraz gromadzą są dane archiwalne. Bezpieczeństwo informacji z racji ilości, różnorodności oraz ważności realizowanych przez straż zadań jest ważna dla całego społeczeństwa.

Bezpieczeństwo państwa, obejmuje problematykę przeciwstawiania się wszelkim zagrożeniom zewnętrznym oraz wewnętrznym dla istnienia oraz rozwoju narodu i państwa. Państwo w trosce o własne bezpieczeństwo narodowe ustala zbiór niezbędnych wartości wewnętrznych, a następnie jego zadaniem staje się ich ochrona przed zagrożeniami. Bez wątpienia do wartości tych możemy zaliczyć: przetrwanie, integralność terytorialną, niezależność polityczną i jakość życia[1].

Rozwój informatyzacji, połączony ze zwiększoną ilością wytwarzania i przetwarzania danych, ale także ułatwienie dostępu do pozyskiwania tych danych z pewnością przyczyniło się do wzrostu zainteresowania systemami zarządzania bezpieczeństwem informacji. Dodatkowo wpływa na to rozwój elektroniki, unitarnych sieci teleinformacyjnych (Internet), powszechność urządzeń dostępowych, a także powstanie społecznościowych sieci i mediów, czy też wykorzystywanie sieci publicznych do przesyłania informacji do systemów przemysłowych. To wszystko sprawia, że informacja staje się kluczowym czynnikiem wyznaczającym wiedzę, władzę, ale i decydującym o bezpieczeń-

[1] J. Janczak, A. Nowak, *Bezpieczeństwo informacyjne…*, op.cit., s. 10-11.

stwie obywateli, organizacji i całych państw[2]. Ponadto wpływ mają także na to takie czynniki jak usprawnienie procesów przekazywania lub pobierania znacznych ilości danych i informacji w niewielkich jednostkach czasu – co w dzisiejszych realiach jest jednym z głównych priorytetów naszego społeczeństwa.

Biorąc pod uwagę powyższe każda organizacja powinna wypracować odpowiednie normy i procedury, które pozwolą tej instytucji odpowiednio przygotować się na zakłócenia związane z brakiem dostępności i integralności lub utratą poufności danych. Analiza tego procesu dokonywana przez specjalistów wielu dyscyplin naukowych określa dalszy kierunek rozwoju jako bazujący na wiedzy i informacji w społeczności globalnej[3].

Zapewnienie bezpieczeństwa systemu informacyjnego w organizacji publicznej, w tym także w Państwowej Straży Pożarnej, powinno być wysoce cenione, gdyż stanowi o sile tej jednostki we współczesnej rzeczywistości i otoczeniu zewnętrznym. Szef każdej jednostki powinien propagować politykę bezpieczeństwa informacyjnego wśród swojej kadry, a racjonalność przy zarządzaniu informacją świadczy o wysokich kompetencjach menedżerskich takiej osoby oraz jest potwierdzeniem i dowodem podążania jednostki za nieustannym rozwojem, który wywołuje ciągłą zmienność potrzeb.

Zaspokajanie potrzeb informacyjnych dokonuje się w ramach procesu informacyjnego, który jako element integrujący i sterujący podstawowymi i pomocniczymi działaniami zmierzającymi poprzez realizację konkretnych zadań do osiągnięcia celów ma również wpływ na skuteczność procesu decyzyjnego[4].

Posiadanie pełnej wiedzy o stanie bezpieczeństwa systemu informacyjnego w badanej organizacji, w razie pewnych niedoskonałości uświadomić może potrzebę zwiększenia działań prewencyjnych w tym zakresie. Zwyczajowo polityka bezpieczeństwa powinna być kreowana przez kierownictwo organizacji, przy wsparciu osób odpowiedzialnych za ochronę informacji znajdujących się w gestii tego podmiotu[5].

Dzisiejsza rzeczywistość zmusza do wnikliwej analizy poziomu bezpieczeństwa systemu informacyjnego w podmiotach sfery publicznej. Jest to konieczne, aby wzmacniać kanały informacji, które nie są należycie chronione, gdzie występuje brak kontroli nad przepływem wszelkiej informacji.

---

[2] K. Liderman, Bezpieczeństwo informacyjne, Wydawnictwo Naukowe PWN, Warszawa 2012, s. 11-12.
[3] Świat w 2025. Scenariusze Narodowej Rady Wywiadu USA, Alfa Sagittarius, Kraków 2009, s. 195-196.
[4] G. Michalczewski, *Czynniki kształtujące potrzeby informacyjne* (w:) *Procesy informacyjne w obronności i bezpieczeństwie. Teoria i praktyka,* pod red. M. Wrzosek, Wydawnictwo Akademii Sztuki Wojennej, Warszawa 2017, s. 47.
[5] K. Liderman, *Bezpieczeństwo informacyjne*. Nowe wyzwania, PWN, Warszawa 2017, s. 129.

W kontekście niniejszego rozdziału przeprowadzone badania miały na celu znalezienie odpowiedzi na pytanie stanowiące ***szczegółowy problem badawczy*** w postaci pytania: *Jak funkcjonuje system bezpieczeństwa wymiany informacji w teorii i praktyce? oraz* **zweryfikowanie przyjętej hipotezy**, która zakłada, że *bezpieczeństwo systemu informacji w Państwowej Straży Pożarnej regulowane jest pośrednio i bezpośrednio źródłami powszechnie obowiązującego prawa w Rzeczypospolitej Polskiej, do których należą między innymi: Konstytucja RP, ustawy, ratyfikowane umowy międzynarodowe, rozporządzenia, akty prawa miejscowego obowiązujące na obszarze działania organów, które je ustanowiły. System bezpieczeństwa wymiany informacji to strategia działania tej formacji w zakresie zapewniania właściwej ochrony pozyskiwanych i przetwarzanych informacji. W teorii strategia ta ma zapewnić ciągłe doskonalenie podjętych działań i procedur w celu optymalizacji ryzyka związanego z naruszeniem poufności danych. Natomiast w praktyce na strategię składają się wszystkie procedury, polityki, regulaminy i instrukcje bezpieczeństwa informacji, które są wdrożone w każdej jednostce organizacyjnej. Informacja jako zasób i narzędzie stanowi podstawę działalności analitycznej. Bez informacji i jej właściwego procedowania w systemie nie ma szans na właściwe, efektywne i szybkie wykorzystanie działalności analitycznej dla zwiększenia bezpieczeństwa państwa i obywateli, a bezpieczeństwo systemu informacyjnego świadczy o wysokim standardzie zarządzania jednostką organizacyjną.*

W celu znalezienia odpowiedzi na postawiony problem badawczy oraz z myślą dokonania weryfikacji przedstawionej hipotezy, zastosowano dwie podstawowe metody badawcze, a mianowicie[6]:

1. teoretyczne:

a) analizę – wykorzystywaną głównie podczas analizy literatury poświęconej badanemu zagadnieniu;

b) syntezę – wykorzystywaną w celu scalenia poszczególnych elementów analizy w całość;

2. empiryczne:

a) sondaż diagnostyczny badania opinii z wykorzystaniem techniki ankiety przy użyciu narzędzia w postaci arkusza ankiety, celem którego będzie poznanie i zbadanie opinii respondentów na temat wpływu określonych czynników na skuteczne funkcjonowanie

[6] Wyjaśnienie zastosowanych metod badawczych zostało ujęte w rozdziale metodologicznym.

organizacji zhierarchizowanej jaką jest formacja Państwowej Straży Pożarnej - w zakresie działania systemu informacyjnego;

b) metodę obserwacji z wykorzystaniem techniki obserwacji przy użyciu narzędzia w postaci arkusza obserwacji – którą wykorzystano w celu rzetelnego utrwalenia jak największej liczby spostrzeżeń autora dysertacji odnośnie do procesów obiegu informacji w organizacji, użytych następnie do rozważań nad sytuacją problemową, stanowiącą wyjście do podjętych badań i sformułowania celu ich przeprowadzenia oraz właściwej interpretacji.

Rzecz jasna to nie jedyne metody badawcze zastosowane podczas analizy zagadnienia, bowiem obok wyżej wymienionych zostały zastosowane również inne metody teoretyczne, a mianowicie:

- abstrahowanie – służące do wyodrębnienia bądź pominięcia określonych elementów badanego zjawiska, które z pewnych przyczyn zostały określone jako bardzo istotne, bądź jako nie mające dla niego znaczenia,
- uogólnienie – wykorzystywane do scalania przedmiotów analizy w oparciu o posiadane przez nie cechy charakterystyczne,
- wnioskowanie – jako działanie mające na celu wypracowanie spostrzeżeń będących przedmiotem analizy jednostki Policji jako organizacji zhierarchizowanej.

2.1 IDEA BEZPIECZEŃSTWA INFORMACYJNEGO W UJECIU TEORETYCZNYM I PRAWNYM

Dopiero od paru dekad rozwijają się badania nad informacją i jej bezpieczeństwem, gdy zaś komunikacja międzyludzka już od tysiącleci jest tematem zainteresowania naszej kultury. Pokazuje to, że informacja staje się uniwersalnym tematem komunikacji i pośrednio powszechnej wiedzy. Istota i czynna rola informacji w życiu jednostek i społeczeństw ujawnia się dopiero przez jej funkcjonowanie w różnych układach komunikacyjnych[7].

W literaturze przedmiotu „Wiek XXI" nazwany jest wiekiem informacji. Pokazał on zmianę natury, rodzaju i charakteru występujących zagrożeń na świecie, gdyż w czasach powszechnego dostępu do technik informatycznych, rodzą się nowe niebezpie-

[7] M. Hetmański, *Świat informacji*, Difin SA, Warszawa 2015, s. 142.

czeństwa[8]. Są one ściśle powiązane z użytkowaniem sieci informatycznych i systemów informacyjnych np. naruszenia/przekroczenia prawa wykorzystujące komputer jako narzędzie, utracenie informacji związana z włamaniami komputerowymi, szeroko rozumiane hackerstwo, złośliwe oprogramowanie i wirusy, szpiegostwem, sabotażem[9].

Odpowiedzią natomiast na przedstawione powyżej zagrożenia stają się takie pojęcia jak rozpoznanie, osiągnięcie, utrzymanie i doskonalenie bezpieczeństwa informacyjnego. Jest to nieodzowne do zapewnienia przewagi konkurencyjnej podmiotów publicznych i gospodarczych w ich płynności finansowej, dochodowości i przede wszystkim pozostawania w zgodzie z literą prawa[10].

Należy zauważyć, iż niebywale do zwiększenia uwagi na problem bezpieczeństwa danych osobowych w jednostkach publicznych przyczyniły się aspekty prawne wynikające chociażby z Konstytucji RP, Rozporządzenia Parlamentu Europejskiego i Rady UE 2016/679 z dnia 27 kwietnia 2016 r. (tzw. RODO) oraz Ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych ze zmianami. Innymi słowy można powiedzieć, że dodatkowym czynnikiem determinującym stały wzrost zainteresowania tematyką bezpieczeństwa informacji są potrzeby dostosowywania organizacji do wymagań mających zastosowanie w przepisach prawa i innych wymagań, których celem jest zapewnienie ochrony określonym grupom interesariuszy.

Zwiększające się zainteresowanie normami w zakresie bezpieczeństwa informacji pozwala na bardziej światłe podejmowanie bieżących decyzji czy też dotyczących inwestycji infrastrukturalnych. Kluczowym i jednocześnie uznawany standardem światowym w tym zakresie jest norma PN-ISO/IEC 27001: 2007 Technika informatyczna - Techniki bezpieczeństwa - Systemy zarządzania bezpieczeństwem informacji - Wymagania ISO 27 001[11].

Zdefiniowanie pojęcia bezpieczeństwa informacji nie jest prostą kwestią, wręcz jest to dość problematyczne. Wpływ ma na to rozwój technologiczny w zakresie intensywnie zmieniającej się informatyzacji naszego życia. Ponadto ciągle pojawiają się coraz to nowe zabiegi i starania mające na celu działania przełamujące już istniejące zabezpieczenia.

[8] Zagrożenie (…) to najbardziej klasyczny czynnik środowiska bezpieczeństwa. Zob., S. Koziej, *Teoria sztuki wojennej*, Bellona, Warszawa 2011, s. 268.
[9] K. Liderman, *Bezpieczeństwo informacyjne…*, op.cit., s. 24.
[10] A. Nowak, W. Scheffs, *Zarządznie bezpieczeństwem*…, op.cit., s. 22.
[11] PN-ISO/IEC 27001:2007, *Technika informatyczna - Techniki bezpieczeństwa - Systemy zarządzania bezpieczeństwem informacji - Wymagania*, PKN, Warszawa 2007.

Próbując przybliżyć pojęcie bezpieczeństwa informacyjnego, należy rozłożyć zestawienie tych słów i odpowiedzieć na pytanie, jak rozumieć pojęcie bezpieczeństwo oraz informacja.

Szeroko pojęte bezpieczeństwo publiczne – bezpieczeństwo obywateli należy do głównych zadań każdego państwa. Podając za literaturą można stwierdzić, że w zasięgu przestrzennym aktywności państwa, można wyodrębnić funkcję wewnętrzną, która obejmuje swoim zasięgiem działania pozwalające zagwarantować bezpieczeństwo i harmonię w danym kraju. Jest to funkcja porządkowa, polegająca na podejmowaniu działań, które zapewniają ład na terytorium państwa[12].

Podstawową rolą państwa jest zapewnienie obywatelom należnych im warunków ochrony przed wszystkimi rodzajami zagrożeń, która realizowana jest poprzez systemy i struktury (w tym instytucje publiczne). Podejmowane przez te instytucje działania powinny być adekwatne ze względu na rodzaj i zasięg zdarzenia. Zabezpieczenie bezpieczeństwa powszechnego, jako jednej z głównych potrzeb występujących w życiu człowieka, to element, który państwo powinno bezwarunkowo i globalnie zagwarantować swoim obywatelom. Jest to bez wątpienia jeden z głównych czynników determinujących jakość współczesnego życia.

Bezpieczeństwo można postrzegać w dwojaki sposób – można je wyrażać zarówno jako stan lub proces[13]. Stan poczucia bezpieczeństwa można określić jako warunki, w których człowiek czuje się „wolnym i zabezpieczonym przed potencjalnymi lub realnymi zagrożeniami, pewnym niezakłóconego bytu i rozwoju, przy pomocy wszelkich dostępnych środków, a także działającym twórczo na rzecz osiągania takiego stanu”[14]. Za pojęciem bezpieczeństwo ogólnego idą takie potrzeby ludzkie i grup społecznych, że stanowią one najważniejszy ich cel[15].

Rozszerzając pojęcie bezpieczeństwa do terminu bezpieczeństwa wewnętrznego państwa należy odnosić to do zagrożeń i przeciwdziałań wobec nich. Natomiast bezpieczeństwo narodowe to stan niezagrożonego spokoju narodu, wyrażany poprzez potrzebę istnienia, przeżycia, gwarancji, a także stałości, tożsamości i niezależności, ochrony poziomu i jakości życia.

---

[12], Encyklopedia Zarządzania – wersja online, hasło *Funkcje współczesnego państwa* (dostęp 2022-09-01).
[13] J. Stefanowicz, *Bezpieczeństwo współczesnych państw*, Wyd. PAX, Warszawa 1984 r., s. 18.
[14] W. Kitler, *Bezpieczeństwo narodowe RP. Podstawowe kategorie. Uwarunkowania*. System, wyd. AON, Warszawa 2011 r., s. 23.
[15] J. Stańczyk, *Współczesne pojmowanie bezpieczeństwa*, wyd. ISP PAN, Warszawa 1996 r., s. 18.

Natomiast przedstawiając bezpieczeństwo jako proces należy podkreślić, iż realizuje się on w złożonym środowisku, a jego konsekwencje odnoszą się nie tylko właściwych osób i grup społecznych, środowisk, regionów i całych narodów, ale obejmują również inne społeczności. Wpływ ma na to, chociażby fakt przestrzennego rozprzestrzeniania się zagrożeń, które nie znają pojęcia "granic państwa" (np. terroryzm, cyberprzestępczość).

Bezpieczeństwo można rozumieć jako stan dający poczucie pewności i gwarancję jego zachowania oraz szansę na doskonalenie[16].

Podając za T. Łoś-Nowak pojęcie to jest trudne do określenia ze względu na fakt, że bezpieczeństwo to nie tylko stan możliwy do określenia jedynie w ustalonym miejscu i czasie, ale także aktywny, zmieniający się w czasie proces[17].

Rozpatrując istotę pojęcia bezpieczeństwa informacyjnego, zasadne jest odniesie się do ogólnej definicji bezpieczeństwa organizacji. Można w tym miejscu posiłkować się stanowiskiem sformułowanym przez S. Kozieja, określającym bezpieczeństwo podmiotu jako proces, czyli tę dziedzinę jego działalności, która zmierza do zapewnienia możliwości przetrwania, rozwoju i swobody realizacji własnych interesów w konkretnych warunkach. Wykorzystując przy tym sprzyjające okoliczności i szanse, podejmując wyzwania, redukując wszelkie ryzyka, a także przeciwdziałając i przeciwstawiając się jakiemukolwiek rodzaju zagrożeń dla podmiotu i płynących dla niego korzyści[18].

W literaturze przedmiotu, napotkać można wiele ujęć terminu "informacja" prezentowanych przez autorów o różnych zainteresowaniach naukowych i jest ona uzależniona od odmienności różnych dyscyplin naukowych np. informacja jako, „nazwa treści zaczerpniętej ze świata zewnętrznego, w miarę jak się do niego dostosowujemy i przystosowujemy doń swoje zmysły. Proces otrzymywania i wykorzystania informacji jest procesem dostosowania się do różnych ewentualności środowiska zewnętrznego oraz naszego czynnego życia w tym środowisku”[19].

Informacja to bodziec oddziaływujący na układ recepcyjny człowieka, powodujący wytwarzanie w jego wyobraźni przedmiotu myślowego, odzwierciedlającego obraz rzeczy materialnej lub abstrakcyjnej, który następnie w jego przekonaniu i świadomości kojarzy się jakoś z tym bodźcem. Oznacza to, że informacje to tylko te doznania, które inspirują

[16] Słownik terminów z zakresu bezpieczeństwa narodowego, wyd. AON, Warszawa 2008 r., s. 14.
[17] T. Łoś-Nowak*, Bezpieczeństwo*, [w:] A. Antoszewski i R. Herbut (red.), *Leksykon politologii*, Alta 2, Wrocław 2003, s. 37-38.
[18] S. Koziej, Teoria sztuki…, op.cit., s. 255.
[19] S. Forlicz, *Informacje w biznesie*, PWE, Warszawa 2008, s. 13.

umysł ludzki do pewnej wyobraźni, Jej istnienie jest relatywnie związane z istnieniem człowieka i jego umysłem[20].

Leszek F. Korzeniowski rozumie bezpieczeństwo informacyjne podmiotu, czyli człowieka lub organizacji jako możliwość pozyskania dobrej, jakości informacji oraz ochrony posiadanej informacji przed jej utratą[21]. Takie stanowisko akceptuje i powiela także uznany badacz problematyki bezpieczeństwa informacyjnego Krzysztof Liderman. Dodaje on jednak, iż bezpieczeństwo informacyjne oznacza uzasadnione zaufanie podmiotu, do jakości i dostępności pozyskiwanej oraz wykorzystywanej informacji[22].

Informacja stanowi także zasadniczy i pierwszoplanowy element przewagi współczesnych konfliktów, w których wykorzystywana jest zarówno, jako broń, jak i traktowana, jako cel. Teoretycy wskazują nawet na konieczność traktowania sfery informacyjnej, jako nowoczesnego środka walki[23].

W literaturze często dochodzi do przyrównywania bezpieczeństwa informacyjnego z bezpieczeństwem informacji. Podając chociażby za K. Liderman bezpieczeństwo informacji jest składową bezpieczeństwa informacyjnego – informację należy najpierw pozyskać, a potem w trakcie jej wykorzystania, przechowywania, przetwarzania, bądź przesyłania odpowiednio i należycie chronić[24].

W Strategii Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej, która stanowi trzon dyrektyw strategicznych dla działalności państwa wskazano natomiast, że bezpieczeństwo informacyjne nie jest tym samym, co bezpieczeństwo informatyczne. Odmienny punkt widzenia odnośnie do pojęcia informacji spotyka się w tzw. semantycznej teorii informacji, gdzie informacja przedstawiana jest jako zbiór wiadomości o faktach, zdarzeniach lub cechach przedmiotów itp. Zbiór ten następnie ujęty jest i podany w takiej formie, że pozwala odbiorcy, niezależnie czy jest to człowiek, czy maszyna odnieść się do zaistniałej sytuacji i podjąć odpowiednie działanie.

Mamy tu przedstawione wyjaśnianie znaczenia pojęcia informacji w aspekcie użytkowym, badaniem i wyjaśnianiem własności informacji, analizą żądań użytkownika, kierowanych pod adresem informacji oraz poszukiwaniem metod i sposobów zaspokojenia przez informację żądań, które formułuje użytkownik[25]. W takim spojrzeniu można zaob-

[20] R. Kawećka, *Informacja w walce zbrojnej*, Wydawnictwo AON, Warszawa 2001, s. 17.
[21] L. F. Korzeniowski, *Podstawy nauk o bezpieczeństwie*, Warszawa 2012, s. 147.
[22] K. Liderman, *Bezpieczeństwo informacyjne*, Warszawa 2012, s. 22.
[23] B. Balcerowicz, *Siły zbrojne w stanie pokoju, kryzysu i wojny*, Wydawnictwo Naukowe Scholar, Warszawa 2010, s. 218.
[24] Ibidem, s. 22.
[25] Bo. Sundgren, An Infological Approach to Data Bases, Urval nr 7, Stockholm 1976.

serwować tak zwaną decyzyjność informacji, czyli jej wpływ na podejmowane przez ludzi decyzje i działania.

W miejscu tym można również wskazać szerokie i wąskie znaczenie tego terminu. W szerokim ujęciu informacja to nie tylko wiadomość, ale także każda decyzja, zakaz, sugestia czy polecenie. Może ona być przekształcana w relacji człowiek-człowiek, ale także w innych systemach, gdzie funkcje nadawcy i odbiorcy mogą pełnić zarówno istoty żywe, maszyny, jak i obiekty.

W wąskim znaczeniu informacja stanowi wiadomość pozyskiwaną przez człowieka na tle obserwacji lub przemyśleń, które podlegają przekazowi w układzie nadawca-odbiorca. Przedstawiając wąskie znaczenie, podając za J. Oleńskim należy wyróżnić dwa podstawowe rodzaje informacji:

- informację jednostkową – przedstawiającą pojedynczy obiekt, proces, zdarzenie w formie [O, C, W], gdzie O – oznacza nazwę obiektu, procesu, określenie zdarzenia jednostkowego, C – to nazwa mierzonej cechy, natomiast W - wartość cechy uzyskana w wyniku pomiaru.
- informację zagregowaną - odnoszącą się do zbiorów obiektów jednostkowych lub zbiorów cech, przy czym łączenie elementów w całość tzw. agregacji można dokonywać: w przestrzeni obiektów, w przestrzeni cech (atrybutów), w przestrzeni obiektów i cech. Dokonuje się to przez: sumowanie, transformację algorytmiczną, translację[26]. Człowiek jest głównym elementem wielorakich procesów informacyjnych, występując na wielu ich etapach, realizującym różnorodne funkcje i zadania. Celem systemu informacyjnego jest natomiast zaspokajanie potrzeb informacyjnych użytkowników, czyli odbiorców informacji, jakimi są kierownictwo różnych szczebli, pracownicy działów itp. Użytkownikiem informacji jest według J. Oleńskiego człowiek, zbiór osób, jednostka organizacyjna lub zbiór jednostek organizacyjnych o zdefiniowanych potrzebach informacyjnych oraz zdefiniowanych sposobach użytkowania informacji, postrzegany w procesie informacyjnym jako jeden odbiorca informacji. Z punktu widzenia procesu informacyjnego jest on postrzegany jako jeden system o celowym działaniu, jego potrzeby są identyfikowane jako jeden zbiór informacji. Użytkownik informacji generuje, gromadzi, przechowuje, przetwarza, przekazuje, udostępnia, interpretuje lub wykorzystuje okre-

[26] J., Oleński, *Ekonomika informacji*. Metody, PWE, Warszawa 2003. s 208-220.

ślone zbiory informacji. Posiada również umiejętność interpretacji wiadomości występujących w danym procesie lub systemie informacyjnym[27].

Wyzwania i zagrożenia bezpieczeństwa systemów informacyjnych wynikające z procesów globalizacyjnych są przedmiotem licznych badań. O potrzebach i związanych z tym problemami utrzymania bezpieczeństwa systemu informacyjnego traktował w swojej książce Winn Schwartau. Pisał on o „walce informacyjnej", którą przedstawił, jako działania ukierunkowane na ochronę, wykorzystanie, uszkodzenie, zniszczenie informacji lub zasobów informacyjnych albo też zaprzeczenie informacjom po to, aby osiągnąć korzyści, jakiś cel lub zwycięstwo nad przeciwnikiem[28]".

Ze względu na różne kryteria klasyfikacji informacji występujących w literaturze, można wyróżnić przedstawione poniżej podstawowe rodzaje informacji[29]:

- Faktograficzna: odwzorowuje wyróżnione stany obiektów w ramach danej obserwacji (obiekty, ich cechy i ich wartości, relacje oraz czas)
- Techniczna: to taka informacja faktograficzna, która odnosi się do obiektów technicznych (np. wyrób, surowiec, maszyna), ich cech, takich jak waga, zużycie, kolor, kształt itp.
- Techniczno-ekonomiczna: to taka informacja faktograficzna, której obiektami są obiekty techniczne, ale ich cechami są charakterystyki ekonomiczne, np. cena, koszt wytworzenia, itp.

Ściśle ekonomiczna: może ona mieć charakter albo mikro- albo makroekonomiczny. W pierwszym wypadku jej odniesieniem jest mikroekonomiczny obraz przedsiębiorstwa (np. zysk, sprzedaż w danym okresie, zadanie inwestycyjne, oprocentowanie lokat i kredytów, itp.). W drugim wypadku informacja odnosi się np. do gospodarki narodowej (np. stopa inflacji, stopy procentowe banku centralnego, itp.)

Jednostkowa: dotyczy konkretnego faktu techniczno-ekonomicznego (np. konkretnej transakcji, osoby, itp.)

Zagregowana: opisuje zagregowane zbiory jednorodnych obiektów (np. ilość wytworzonych samochodów w danym czasie) lub ilość takich obiektów mających wspólną cechę (np. ilość sprzedanych samochodów określonej marki). Agregacja może wymagać algorytmów o dużym stopniu skomplikowania.

---

[27] Ibidem, s. 104.

[28] W. Schwartau, *Information Warfare*, New York 1994. Por.: P. Bączek, *Zagrożenia informacyjne a bezpieczeństwo państwa polskiego*, Wydawnictwo Adam Marszałek, Toruń 2005, s. 132.

[29] Encyklopedia zarządzania-wersja online, hasło *rodzaje informacji,* (dostęp 2022-08-10)

Cyfrowa: to informacja przedstawiona w postaci słów cyfrowych (ciągu liczb binarnych składających się z cyfr 0 i 1.)

Indywidualna/adresowana: to informacja, która jest skierowana bezpośrednio do określonego użytkownika. Udzielenie takiej informacji zazwyczaj występuje w postaci rozmowy "konwersacji" bądź korespondencji.

Zbiorowa/powszechna: jest skierowana do wszystkich użytkowników interesujących się danych zagadnieniem. Przekazywanie tej informacji odbywa się bez osobistego udziału osób.

Dokumentacyjna: to informacja pośrednia, wskazuje potencjalne źródła informacji (książki, dokumenty), w których użytkownik może znaleźć informacje.

Faktograficzna (rzeczowa, bezpośrednia): jest to końcowa informacja poszukiwana przez użytkownik, opracowana na podstawie różnych źródeł. Zazwyczaj występuję w postaci tabelek, wykresów, schematów.

Retrospektywna (jednorazowa): dotyczy informacji pochodzących z dowolnego okresu, dostarczona na jednorazowe zapotrzebowanie użytkownika.

Bieżąca (ciągła): ma za zadanie zwrócić uwagę użytkownika na nową informację z określonej dziedziny. Dotyczy ona aktualnych źródeł informacji pierwotnej, najczęściej dotyczy określonego okresu np. za trzy ostatnie miesiące. Jest ona dostarczana systematycznie użytkownikowi.

Kolejnym charakterystycznym przykładem definicji informacji będzie jej ujęcie inżynierskie jako klasyczna teoria informacji, czyli dyscypliny zajmującej się problematyką informacji oraz metodami przetwarzania informacji, np. w celu transmisji lub kompresji. Za jej ojca uznaje się matematyka i inżyniera Claude E. Shannon, który poruszył jej temat w swoim dziele Amathematical theory of communication opublikowanym w czasopiśmie Bell System Technica Journal, w 1948 roku.

Czasami opisywana jest ona jako teoria przekazywania wiadomości za pomocą sygnałów, opartej na teorii funkcji decyzyjnych[30].

Charakterystyczne dla teorii informacji jest to, że informacja traktowana jest jako najistotniejszy składnik każdego systemu. Za pomocą informacji można określić stopień zorganizowania masy oraz energii w systemie, natomiast szczególne znaczenie informacja ma w systemach cybernetycznych.

[30] J. Nowakowski, W. Sobczak, *Teoria informacji*, Wydawnictwo Naukowo-Techniczne, Warszawa 1970, s 9.

Informacja to dowolna wiadomość, na podstawie której odbiorca wiadomości opiera swoje działanie[31].

W teorii tej należy rozumieć trzy pojęcia[32]:

- informacja,
- system,
- entropia.

Każdy system posiada określoną strukturę, a informację, która związana jest bezpośrednio ze strukturą systemu nazywamy informacją strukturalną. Ponadto w teorii informacji wyróżnia się informację względną, która związana jest z komunikacją systemów.

Entropia to miara nieokreśloności na potrzeby cybernetyki. W teorii systemów jest miarą uporządkowania. Im wartość entropi jest mniejsza tym system jest bardziej uporządkowany, a wraz ze wzrostem wartości entropi spada jego uporządkowanie. Poziom najwyższy oznacza że mamy do czynienia z chaosem, natomiast zerowa entropia oznacza system doskonale uporządkowany, w którym można stwierdzić zdarzenia z prawdopodobieństwem równym jedności. W momencie, w którym oczekiwane zdarzenie ma miejsce, zmniejsza się poziom niewiedzy i niesie to pewną informację. Informacja wypiera tutaj pewien poziom entropii. Dzięki temu można uznać entropię za miarę informacji[33].

Wartość entropii przedstawia się następującym wzorem[34]:

$$H(p) = -\sum_{i=1}^{n} p_i log p_i$$

gdzie:

H(p) - nieokreśloność zajścia zdarzenia,

p - prawdopodobieństwo zajścia niezależnego zdarzenia.

Informacja może być rozpatrywana w trzech aspektach:

[31] Ibidem, s.10.
[32] S. Mynarski (red.) *Elementy teorii systemów i informacji*, Akademia Ekonomiczna w Krakowie, Kraków 1989. S 146.
[33] S. Mynarski (red.) Elementy teorii systemów i informacji, Akademia Ekonomiczna w Krakowie, Kraków 1989, s. 147.
[34] Ibidem, s. 149.

- ilościowym - oznacza ilość sygnałów i symboli, które są niezbędne do jej przekazania,
- znaczeniowym - związany jest z interpretacją treści i komunikowaniem się nadawcy z odbiorcą,
- wartościowym - ma na celu pokazanie użyteczności przekazanej informacji.

C. F. Shannon formułując teorię informacji stworzył również matematyczne podstawy teorii kodowania, co wykorzystywane jest w[35]:

- sferze przechowywania informacji,
- realizacji rożnego typu systemów sterowania,
- projektowaniu i budowie systemów automatycznego sterowania.

W tej formule informacja jest ściśle związana z teoretyczną koncepcją "systemu komunikacyjnego", w którym występują następujące elementy:

- źródło wiadomości,
- koder,
- kanał,
- dekoder,
- odbiorca wiadomości oraz szum.

Teoria informacji jest to dziedzina nauki, która za pomocą modelu matematycznego opisuje poszczególne elementy "systemu komunikacyjnego"[36].

W teorii systemów i cybernetyce informacja występuje obok materii i energii jako jeden z trzech zasadniczych elementów wymiany pomiędzy układami względnie odosobnionymi a otoczeniem. Wymiana ta ma postać powiązań informacyjnych skierowanych albo z otoczenia do wyodrębnionego układu, albo z układu do otoczenia. Głównym zadaniem każdego systemu jest transformacja, czyli przetwarzanie zasileń materialnych, energetycznych i informacyjnych znajdujących się na wejściach systemu w odpowiednie wyjścia materialne bądź też informacyjne[37].

Ponadto w cybernetyce informacja określona została w dwojaki sposób i występuje w ujęciu realnym i abstrakcyjnym. W określeniu realnym dotyczy systemu, struktury i stopnia jego zorganizowania. Natomiast w ujęciu abstrakcyjnym dotyczy przedmiotów, zdarzeń lub wytworów umysłu. Szczególnie istotne jest tutaj zespolenie pomiędzy materią,

[35] Z. Łukasik, *Teoria informacji i sygnałów,* Wydawnictwo Politechnika Radomska, Radom 2004, s. 65-68.
[36] Ash R.B., *Information Theory, Dover Publications*, Inc., New York 1990, s. 1-2.
[37] S. Mynarski, *Elementy teorii systemów i cybernetyki*, PWE, Warszawa 1979, s. 9-10.

energią i informacją. Informacja jest uznana za najważniejszy składnik każdego systemu, gdyż wprowadza ład i uporządkowanie[38].

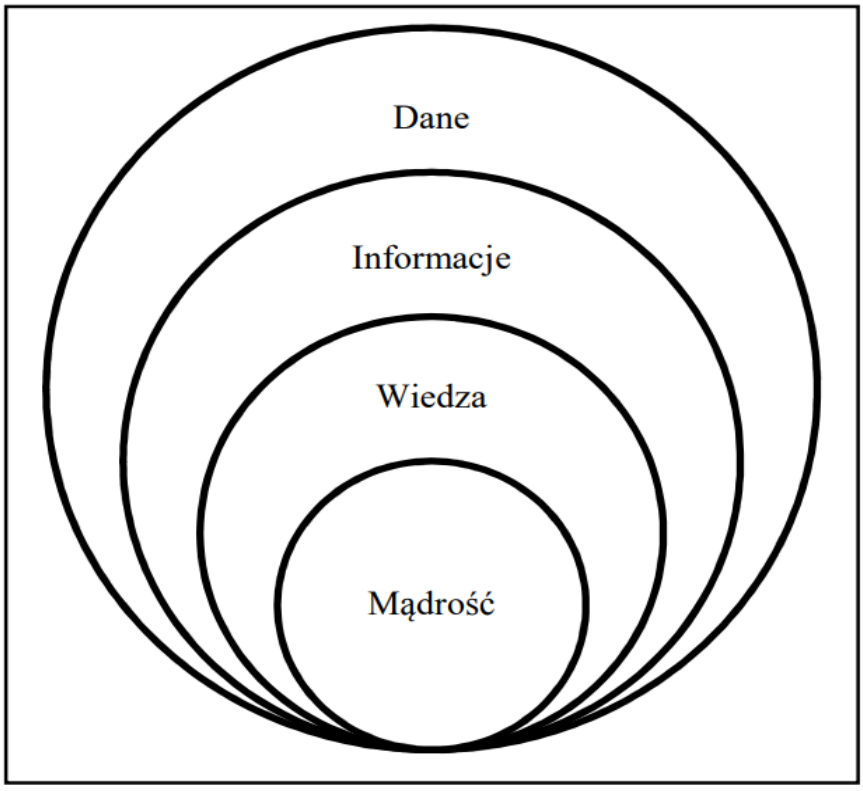
Wspominając w tym miejscu o transformacji, czyli przetwarzaniu danych jako jednym z głównych zadań systemu informacyjnego należy wymienić podstawowe formy przetwarzania danych, jakimi są np.:

- klasyfikacja danych,
- sortowanie danych,
- agregacja danych,
- przeprowadzanie obliczeń z wykorzystaniem danych
- selekcja danych.

Swoiste znaczenie pojęcie informacja nabiera, gdy poddamy je analizie w kontekście zarządzania przedsiębiorstwem, czy też instytucją publiczną. Rzeczowa i realistyczna teoria informacji opiera się właśnie na analizie i ocenie walorów poznawczych i użyteczności różnego rodzaju danych dla osób zarządzających organizacjami, co wpływa na efektywność podejmowanych decyzji. Zauważyć tu można, że informacja często traktowana jest jako szczególnego rodzaju zasób przedsiębiorstwa, który jest niezbędny do osiągania istotnej przewagi konkurencyjnej. Następnie każdy zasób powinien podlegać analizie i ocenie osób zarządzających z punktu widzenia jego przydatności do realizacji celów danej instytucji. Niewątpliwie informacja jest nierozłączną cechą pracy każdego menedżera, a jej znaczenie jako potrzeba zarządzania nią, coraz szybciej wzrasta. Ponadto jej rosnące znaczenie wynika z coraz większej złożoności otoczenia, w jakim działają organizacje i coraz większej masy informacji, która ta złożoność rodzi.

Informacja jest ważną częścią komunikacji, a zarządzanie nią jest nieodzowną cechą tego procesu. Zarządzanie można opisać jako szereg etapów obejmujących odbiór, przetwarzanie i upowszechnianie informacji. Szefowie poszczególnych instytucji otrzymują dane i następnie muszą zdecydować, co z nimi robić. Niektóre z nich zatrzymywane są do dalszego użycia w formie w jakiej zostały pozyskane, podczas gdy inne informacje grupuje się i przekształca tak, by utworzyły nową informację. Kolejno pewne informacje używa się niezwłocznie i bezpośrednio, a niektóre przekazuje się innym pracownikom do realizacji. Natomiast pewne dane uznawane są za niepotrzebne i nic nie wnoszące do pracy, zadań i celów danej instytucji i po prostu się je odrzuca.

[38] Ibidem, s. 140.



Źródło: Waldemar Krztoń, *XXI WIEK – WIEKIEM SPOŁECZEŃSTWA INFORMACYJNEGO, MODERN MANAGEMENT REVIEW*, str. 105.

Rysunek 2-1
Hierarchia informacji

Podając za M. Wrzosek do opisywania informacji wykorzystuje się następujące zasadnicze terminy: dane, informacje, wiedzę i mądrość, gdzie[39]:

- dane to uporządkowany zbiór nazw i wartości liczbowych opisujących określony obiekt (system, proces, zdarzenie);
- informacje to zbiór danych uporządkowanych zgodnie z potrzebami odbiorcy (użytkownika), wyrażającymi jego potencjalne (lub realne) działania;
- wiedza to zbiór informacji wykorzystywanych przez użytkownika zgodnie z wymogami w podejmowanych działaniach;
- mądrość to wiedza, dzięki której podmiot (użytkownik) realizuje swoje cele zgodnie z przyjętym systemem wartości.

W tym miejscu należy przedstawić zróżnicowanie pomiędzy danymi i informacjami.

[39] M. Wrzosek, *Procesy informacyjne w zarządzaniu organizacją zhierarchizowaną*, Warszawa 2010, s. 30.

Dane to surowe, nie obrobione liczby i fakty odzwierciedlające jakiś jeden aspekt rzeczywistości. Natomiast informacja to dane przedstawione w sposób mający jakieś znaczenie. Zarządzanie informacją jest traktowane jako istotna część procesu kontroli w organizacji. Menedżerowie otrzymują znacznie więcej danych i informacji niż potrzebują czy są w stanie wykorzystać, a właściwa decyzja o sposobie ustosunkowania się do otrzymanej informacji jest ze swojej istoty formą kontroli.

W. Flakiewicz wskazuje w swoich opracowaniach różne rodzaje użytkowników informacji[40].

- użytkownik potencjalny - który z różnych przyczyn, zarówno obiektywnych jak i subiektywnych, nie jest zainteresowany daną informacją,
- użytkownik przypuszczalny - mający bezpośredni lub pośredni dostęp do określonej informacji,
- użytkownik rzeczywisty - osoba, posługująca się daną informacją w ramach swoich obowiązków służbowych,
- użytkownik korzystający – ten, który wynosi bezpośrednią korzyść z posiadanej informacji, z racji jej użycia w określonym celu.

Jeżeli natomiast na organizację spojrzymy jako ustrukturalizowany, czyli uporządkowany w pewien sposób systemem (całość), to możemy wyłonić wówczas złożone z czterech podstawowych elementów (podsystemów) grupy użytkowników wewnętrznych informacji:

- kierownictwo najwyższego szczebla: odpowiadający za decyzje strategiczne.
- kierownictwo średniego szczebla: szczebel taktyczny.
- kierownicy bezpośrednio nadzorujący pracę, czyli szczebel operacyjny.
- wykonawcy: zwykle stanowiący najliczniejszą grupę użytkowników informacji.

Pominięcie jakiejkolwiek z grup użytkowników przedstawionych powyżej naraża instytucję na duże trudności w eksploatacji systemu. Należy pamiętać, że użytkownicy informacji to najważniejszy element całego systemu, a przygotowanie i przeszkolenie ich wszystkich ma decydujący wpływ na to, czy system będzie efektywny. Samo użycie najnowszego sprzętu informacyjnego i oprogramowania nie przyniesie zamierzonego efektu, jeżeli personel nie będzie na najwyższym, profesjonalnym poziomie.

Komunikacja użytkownika informacji z systemem informacyjnym musi być procesem iteracyjnym. Posiadacza informacji nie zawsze satysfakcjonuje pierwsza odpowiedź,

[40] W. Flakiewicz, *Systemy informacyjne w zarządzaniu*, Warszawa 2012 rok, s.28.

dla uściślenia i uzyskania odpowiedzi końcowej zadaje on dodatkowe pytania. Również z podobnym sposobem działania spotykamy się, jeżeli pytanie użytkownika jest nieprecyzyjne lub wieloznaczne[41].

Niezmiernie istotny wpływ na użytkowników informacji, jak i samego systemu informacyjnego ma otoczenie:

- organizacje współdziałające,
- organizacje nadrzędne,
- klienci,
- inni.

Podając za literaturą w przedsiębiorstwie można wymienić następujące rodzaje informacji[42]:

- Zewnętrzne - (np. wielkość sprzedaży konkurentów, zachowania nabywców)
- Wewnętrzne- (np. wielkość sprzedaży, poziom i struktura kosztów, itp.)
- Wtórne- to takie, które już istnieją, zostały przez kogoś wcześniej zgromadzone i opracowane
- Ilościowe - występują w postaci liczbowej
- Jakościowe - występują w postaci opisów
- Z przeszłości - dotyczą jedynie okresu przeszłego (ex post)
- Bieżące - dotyczą teraźniejszości
- Prognostyczne - dotyczą jedynie przyszłości (ex ante)
- Decyzyjne - służą do określenia konkretnych decyzji
- Kontrolne - pomagają w kontroli
- Koordynacyjne - bezpośrednio związana z uczestnikami rynku
- Planistyczne - służą do przewidywania zjawisk w przedsiębiorstwie
- Makroekonomiczne - dotyczą rynku krajowego oraz światowego
- Mikroekonomiczne - dotyczą gospodarstw domowych
- Formalne - są zapisywane na dysku twardym komputera, papierze
- Nieformalne - zdobywanie ich wymaga osobistego zaangażowania
- Operatywne - "są wykorzystywane do podejmowania bieżących decyzji dotyczących powtarzających się działań rynkowych"

[41] M. Kocójowa, *Użytkownicy informacji elektronicznej*, Wydawnictwo Uniwersytetu Jagiellońskiego, Kraków 2000 rok, s 55-78.
[42] Encyklopedia zarządzania-wersja online, hasło *rodzaje informacji,* (dostęp 2022-06-14).

- Specjalne - pozwalają nam przewidzieć reakcje klientów, w wyniku działań jakie stosuje firma

Natomiast kiedy mówimy o cechach użytecznej informacji pod względem zarządzania nią przez menadżera, to taka informacja powinna być:

- Aktualna – musi być łatwa do uzyskania wtedy, kiedy może być bazą odpowiednich działań menedżera, ale nie musi to wcale oznaczać, że powinna być ona dostarczona natychmiast. Jest funkcją sytuacji, w jakiej znajduje się menedżer.
- Dokładna – powinna mieć dla menedżera realną wartość, więc musi być dokładna. Taka informacja zapewnia rzetelne odzwierciedlenie rzeczywistości.
- Odpowiednia – czyli informacja, która jest użyteczna dla menedżera, w zależności od jego konkretnych potrzeb i warunków.
- Kompletna– informacja kompletna dostarcza menedżerowi wszystkich niezbędnych podczas jego pracy faktów i szczegółów. Jeśli informacja ma być użyteczna to obraz sytuacji musi być pełny. Jeśli informacja jest niepełna, menedżer może sobie wyrobić niedokładny lub zniekształcony obraz rzeczywistości.

W odniesieniu do rozeznania i prowadzenia poszukiwań na temat poczucia bezpieczeństwa systemu informacyjnego warto wziąć także pod uwagę schemat zaprezentowany przez D. Freia, w którym uwzględnił on następujące cztery elementy:

- stan braku bezpieczeństwa – gdy występuje rzeczywiste i istotne zagrożenie zewnętrzne, które postrzegane jest, jako adekwatne;
- stan obsesji – 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[43].

Niewątpliwie trzonem bezpieczeństwa informacyjnego jest to, że przechowywane w bazach danych informacje, powinny podlegać ochronie. Dotyczy to głównie danych o kluczowym znaczeniu dla funkcjonowania danego przedsiębiorstwa, czyli tzw. informacji o charakterze strategicznym. Projekt systemu bezpieczeństwa informacyjnego wspierający zarządzanie strategiczne podmiotu, powinien brać pod uwagę problematykę bezpie-

[43] K. Liedel, *Bezpieczeństwo informacyjne w dobie terrorystycznych i innych zagrożeń bezpieczeństwa narodowego*, Wydawnictwo Adam Marszałek, Toruń 2008, s. 8.

czeństwa informacji, poprzez określenie całokształtu, metod i narzędzi ochrony i nadzoru nad informacją.

Zatem do klarownego sprecyzowania i sformułowania definicji bezpieczeństwa informacyjnego potrzebne jest jego ścisłe powiązanie z określeniem atrybutów bezpieczeństwa do których można zaliczyć:

- autentyczność – oznacza, że tożsamość podmiotu lub zespołu jest taka jak deklarowano;
- poufność – wskazuje, że informacja nie jest dostępna dla nieautoryzowanych osób, podmiotów lub procesów;
- integralność danych – ta właściwość oznacza, że dane nie zostały zmienione lub zniszczone w sposób nieautoryzowany;
- dostępność – daje możliwość wykorzystania danych przez osobę, która ma do tego prawo;
- niezawodność – spójne, zamierzone zachowanie i skutki;
- integralność – integralność danych oraz systemu;
- integralność systemowa – właściwość umożliwiająca systemowi realizację zamierzonej funkcji w nienaruszony przez nieautoryzowane manipulacje (celowe lub przypadkowe) sposób;
- rozliczalność - oznacza, że działania podmiotu np. użytkownika mogą być mu przypisane[44].

2.2 ZAGROŻENIA BEZPIECZEŃSTWA INFORMACYJNEGO W INSTYTUCJACH PUBLICZNYCH

Wzrost roli informacji we współczesnym świecie, powoduje wzrost zagrożeń jej bezpieczeństwa[45]. Współczesny włamywacz, nie forsuje już za pomocą łomu pancernych drzwi do bankowego skarbca, ale wykorzystując swoją wiedzę informatyczną, łamie kody dostępów do kont bankowych, z których bez użycia siły fizycznej transferuje środki pie-

[44] J. Czekaj, *Podstawy zarządzania informacją*, Wydawnictwo Uniwersytetu Ekonomicznego w Krakowie 2012, s. 126-129.

[45] A. Nowak, W. Scheffs, *Zarzadzanie*…, op.cit., s. 22.

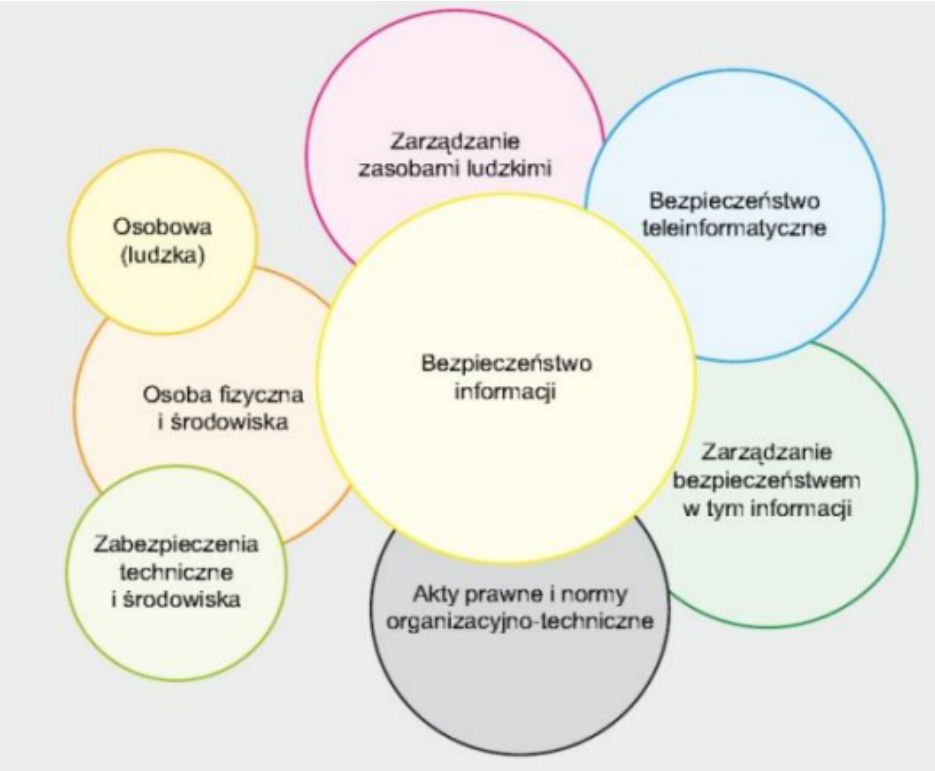
nieżne na wskazane rachunki bankowe[46]. Czasy nam współczesne, do tradycyjnych zagrożeń informacyjnych jak np. szpiegostwo dołożyły nowe, wynikające z rozwoju technologii, tj. przestępstwa komputerowe, cyberterroryzm, a kolejne wyzwania związane z postępem technologicznym mogą stać się źródłem nieznanych dotąd niebezpieczeństw.[47] Zatem zdefiniowanie źródeł zagrożeń bezpieczeństwa informacyjnego wydaje się kluczowe dla zapewnienia bezpieczeństwa informacyjnego organizacji[48].

Starając się przybliżyć problematykę zagrożeń bezpieczeństwa informacyjnego należy przede wszystkim odpowiedzieć na pytanie czym jest zagrożenie i jak je rozumieć. Podając za literaturą przedmiotu zagrożenie to generowane przez czynniki zewnętrzne wobec organizacji, ryzyko ograniczenia możliwości działania na rynku lub poniesienia strat[49]. Należy w tym miejscu zwrócić uwagę i odróżnić pojęcie ryzyka od określenia słabych stron danej instytucji czy podmiotu. Źródło tych drugich znajduje się wewnątrz firmy i także negatywnie wpływa na jej wyniki. Niebezpieczeństwem/zagrożeniem w rozumieniu zarządzania strategicznego, są zawsze czynniki znajdujące się poza organizacją. To coś na co kierownictwo danego podmiotu nie ma ani pośredniego, ani bezpośredniego wpływu. Są to elementy i determinanty, które mogą zmienić się w nieoczekiwany i negatywny sposób w kierunku bez powiązania z działaniami przedsiębiorstwa.

Bez wątpienia, za najbardziej narażone i wrażliwe współczesne dziedziny życia na zagrożenia bezpieczeństwa informacyjnego, a co za tym idzie nieuprawnionym ujawnieniem informacji uznać należy takie obszary jak: planowanie polityczne, zarządzanie w skali makroekonomicznej, polityka obronna, wywiad i kontrwywiad wojskowy itd.

Zagrożenia wobec przedsiębiorstwa mają zawsze charakter negatywny, czy wręcz wrogi i należy je monitorować wśród otoczenia, tak aby należycie wcześnie je dostrzegać i podejmować właściwe działania ochronne i zabezpieczające, pozwalając zapobiegać przed wystąpieniem ich negatywnych skutków.

[46] L. Więcaszek-Kuczyńska, *Obronność*. Zeszyty Naukowe 2(10) /2014, s. 2.
[47] Upływ czasu nie zdezaktualizował koncepcji Sun Tzu: Tego, że się wie zawczasu, nie można uzyskać od duchów (…) ani z gwiezdnych wyliczeń. (…) Do tego trzeba szpiegów. Zob., Sun Tzu, *Sztuka Wojenna*, przeł. Robert Stiller, Vis-a vis Etiuda, Kraków 2011, s. 127.
[48] P. Bączek, *Zagrożenia informacyjne a bezpieczeństwo państwa polskiego*, Wydawnictwo Adam Marszałek, Toruń 2006, s. 7.
[49] Encyklopedia zarządzania - wersja online, hasło *Ryzyko działań na rynku* (dostęp 2023-01-23).



Źródło: *https://www.zabezpieczenia.com.pl/ochrona-informacji/system-zarządzania-bezpieczeństweminformacji-zgodny-z-isoiec-27001-cz-1*

Rysunek 2-2
Zasada synergii systemu bezpieczeństwa informacji

W zależności od rodzaju źródła i czynnika występującego otoczenia wokół przedsiębiorstwa zagrożenia można podzielić na[50]:

- Polityczne, do których zaliczyć możemy między innymi:
  - Przejęcie władzy w kraju przez siły polityczne sprzyjające ograniczaniu praw i wolności gospodarczej.
  - Negatywna ocena branży, w której działa przedsiębiorstwo i nałożenie przez rząd dodatkowych obciążeń podatkowych lub ograniczenie zakresu działania.
  - Otoczenie i klimat polityczny panujący w kraju nie sprzyja budowaniu współpracy i zaufaniu pomiędzy biznesem i jednostkami administracji publicznej.
  - Niepokoje społeczne w kraju i grożące widmo rozruchów, zmniejszają popyt na dobra i usługi.
  - Polityka obciążeń celnych i podatkowych zakłada ich zwiększanie, gdyż rząd musi zrównoważyć budżet.

[50] A. Learned, C. Christensen, Andrews, R. S. and Guth, D. Business Policy: Text and Cases, Homewood (1965), Illinois: Irwin.

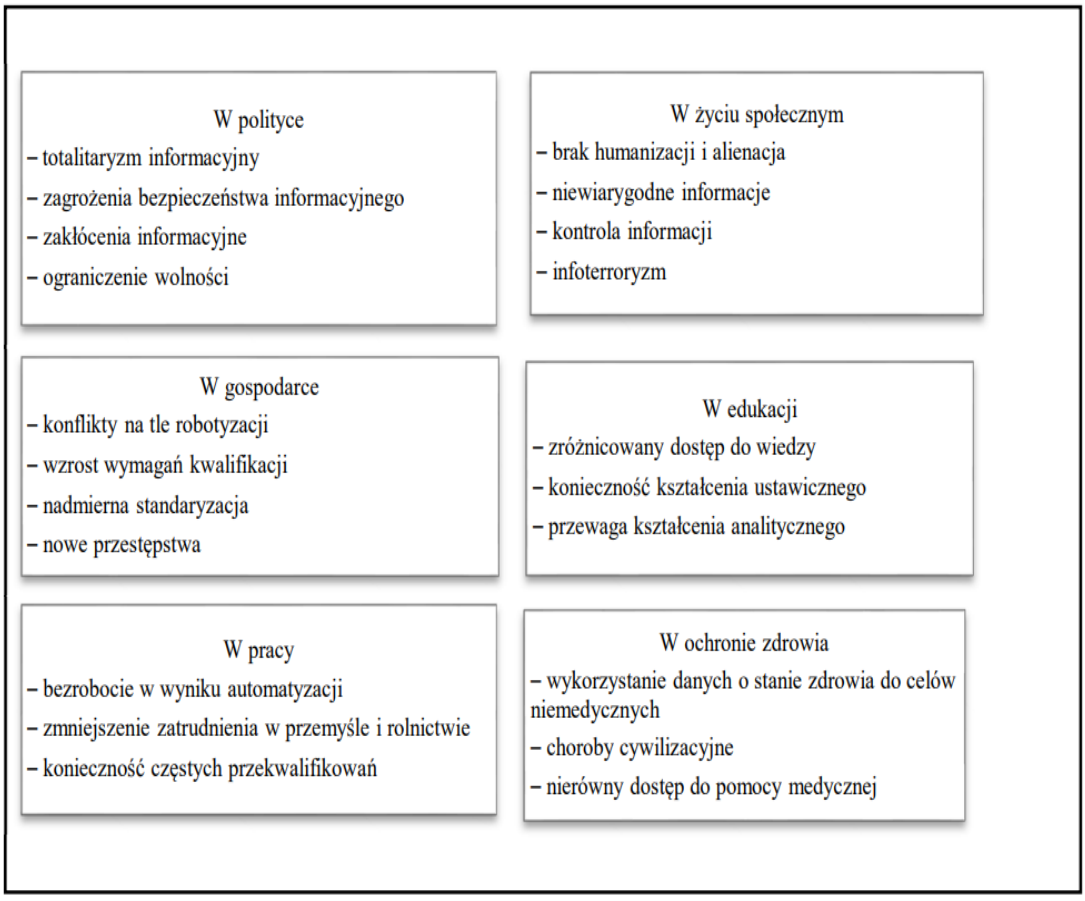
- Występowanie gwałtownych zmian na arenie politycznej - największe partie tracą swoją pozycję na rzecz nowych populistycznych organizacji, głoszących niejednokrotnie hasła ekstremistyczne.

- Ekonomiczne, do których zaliczyć możemy między innymi:
  - Integrację gospodarczą powodującą, że coraz więcej konkurentów zagranicznych zaczyna bez przeszkód działać na rynku lokalnym.
  - Zmniejszenie popytu na produkty i usługi w branży, w której działa firma.
  - Wejście na rynek dużej konkurencji z uwagi na jego rosnącą rentowność i perspektywy dalszego dynamicznego wzrostu.
  - Generowanie przez konkurencję nowych innowacyjnych produktów, które zaspokajają dotychczas niewystępujące potrzeby klientów.
  - Rosnące stopy procentowe, co za tym idzie mniejsza dostępność kredytów, czy podnoszone koszty pozyskania kapitału inwestycyjnego na rozwój.
  - Utrzymująco się na wysokim poziomie inflacja, co ogranicza możliwość długofalowego planowania zakupów, sprzedaży i projektów inwestycyjnych.
  - Niekorzystne kursy walut ograniczają opłacalność eksportu, powodują spadek poziomu rozwoju gospodarczego, co generuje różnego rodzaju kryzysy i niepewność dotyczącą przyszłości.
  - Istnieje realna groźba pojawienia się na rynku substytutów produkowanych produktów i usług, o lepszych parametrach jakościowych i niższej cenie.
- Społeczno-kulturowe, do których zaliczyć możemy między innymi:
  - Rosnące wymagania klientów spowodowane globalizacją.
  - Generowanie przez sieci społecznościowe „mody" na produkty i usługi, w której działa firma, ale którą trudno uzyskać.
  - Zmniejszenie popytu na produkty i usługi oferowane przez firmę ze względu na zmieniający się profil demograficzny ludności lub niż demograficzny przekładający się na potencjalny długoterminowy spadek popytu.
  - Występowania negatywnego nastawienia dotyczącego oceny sytuacji zarówno gospodarczej, jak i różnego rodzaju perspektyw w przyszłości, co prowadzi do tego, że ludzie obawiają się pogorszenia sytuacji gospodarczej, utraty pracy i źródła dochodów.

- Prawne, do których zaliczyć możemy między innymi:
  - Utrudnienie działalności branżowej poprzez ciągle zmieniające się przepisy prawne.
  - Pojawiająca się konieczność uzyskiwania nowych zgód, koncesji, pozwoleń na działalność w branży.
  - Zwiększanie ograniczeń wynikających z prawa pracy.
  - Zwiększanie się obciążenia prawnych związane z funkcjonowaniem związków zawodowych.
  - Wprowadzanie coraz to nowych podatków, bądź para podatków.
  - Działalność związana ze zwiększeniem funkcjonowania organów siłowych: Policja, kontrola skarbowa, kontrola celna, co może prowadzić do kontroli skutkujących zakłóceniami biegu procesów biznesowych.
- Środowiskowe, do których zaliczyć możemy między innymi:
  - Występowanie procesów prowadzących do zwiększania zanieczyszczeń środowiska, co powoduje wzrost kosztów funkcjonowania firmy.
  - Ograniczenia nakładane na firmy korzystające ze środowiska, zwiększają koszty działania i obniżają pozycję konkurencyjną w stosunku do firm, z krajów, gdzie nie ma wyraźnej presji na ochronę środowiska.
  - Ograniczenia wynikające z prawa ochrony środowiska negatywnie wpływają na sprzedaż dotychczas produkowanych, tradycyjnych wyrobów,
- Technologiczne, do których zaliczyć możemy między innymi:
  - Utrudnienie dostępu do innowacyjnych technologii, poprzez posiadanie przez firmy zagraniczne patentów na kluczowe rozwiązania, co nie pozwala na rozwój innowacyjnych produktów i sprawia konieczność ponoszenie bardzo dużych kosztów zakupu tych patentów.
  - Ciągle zwiększający się trend do technologii automatyzujących procesy, powoduje iż produktywność firm konkurencyjnych oraz ich koszty produkcji spadają.
  - Podejmowanie współpracy przez różnego rodzaju jednostki naukowo-badawcze przy wdrażaniu nowych technologii z firmami konkurencyjnymi.
  - Organizowanie się w tzw. klastry technologiczne, skupiające większość firm konkurencyjnych z branży.
  - Utrudnione jest uzyskanie wsparcia w postaci dotacji na utworzenie centrów, czy też projektów badawczo-rozwojowych,

- Procesy, w których szybkość zmian technologicznych powoduje, iż park maszynowy staje się przestarzały zanim zdąży się zamortyzować – skracanie cyklu życia produktów.

Każde postępowe i nowatorskie podejście modernizacyjne czy innowacyjne wpływa na określone skutki społeczne, gospodarcze, ekonomiczne czy kulturowe. Doświadczenia związane z bezpieczeństwem informacji pokazują, że obok występujących zjawisk o charakterze pozytywnym występują zjawiska o wyraźnie negatywnym charakterze. Zagrożeniami w tym obszarze są nowe formy uwarstwienia społecznego, czyli podziału społeczeństwa pod kątem dostępu do informacji, wiedzy, wykształcenia, kwalifikacji. Obecnie znaczący stopień w pozycji społecznej mają umiejętność posługiwania się i wykorzystania technik teleinformacyjnych i dostępu do nich. Proces ten w czasach globalizacji może mieć znacznie większy zasięg, może obejmować nie tylko niektóre grupy społeczne danego państwa, ale także całe społeczeństwa lub państwa.



Źródło: Waldemar Krztoń, *XXI WIEK – WIEKIEM SPOŁECZEŃSTWA INFORMACYJNEGO, MODERN MANAGEMENT REVIEW,* str. 110.

Rysunek 2-3
Zagrożenia występujące w społeczeństwie informacyjnym

W literaturze przedmiotu specjaliści zwracają uwagę na to, że nowe technologie, obok zjawisk korzystnych, mogą być stosowane do wykonywania zadań niejawnych, chociażby takich jak sposobność do manipulacji. Zagrożenia te mogą być stosowane przez różne grupy interesu mające dostęp i możliwość wykorzystywania tych metod. Bazując na ich potencjale, mogą oddziaływać na daną społeczność, tworząc pożądane zachowania społeczne. Funkcje negatywne mogą dotyczyć podejmowania działań przestępczych, takich jak: hackerstwo, rozpowszechnianie rasizmu, szerzenie pornografii nieletnich, propaganda terroryzmu, działania sekt itp.[51].

Rozwój społeczeństwa informacyjnego może być przyczyną zagrożeń, do których z pewnością należy zaliczyć:

- w obszarze polityki dążenie do „totalitaryzmu informacyjnego" - państwowego monopolu, wrażliwość na zakłócenia informacyjne, wrażenie ograniczonej wolności i prywatności;
- w obszarze gospodarki możliwość wystąpienia konfliktów na tle automatyzacji i robotyzacji, redukcję zatrudnienia, wzrost wymagań dotyczących obsługi systemów zautomatyzowanych, nadmierną standaryzację wyrobów i usług, możliwość nowych przestępstw;
- w obszarze życia społecznego: dehumanizację i alienację, zalew niewiarygodnymi informacjami, zmniejszenie prywatności przez zwiększenie i łatwiejszą kontrolę;
- w obszarze pracy: zwiększenie bezrobocia poprzez automatyzację pewnych stanowisk pracy, zmniejszenie zatrudnienia w przemyśle i rolnictwie, powiększenie luki pokoleniowej, konieczność częstych przekwalifikowań;
- w obszarze edukacji i wiedzy: zróżnicowanie dostępu do wiedzy, konieczność kształcenia ustawicznego, kopiowanie prac, załamanie kontroli praw autorskich;
- w obszarze ochrony zdrowia: dehumanizację służby zdrowia, wykorzystanie danych o stanie zdrowia do celów pozamedycznych, nowe choroby cywilizacyjne, zróżnicowanie dostępu do pomocy medycznej[52].

Bezpieczeństwo informacji należy rozpatrywać w trzech zależnych od siebie obszarach:

- bezpieczeństwo informacji obejmującej zasób strategiczny państwa,
- bezpieczeństwo krytycznej infrastruktury teleinformatycznej,

[51] W. Krztoń, *XXI WIEK – Wiekiem Społeczeństwa Informacyjnego*, Modern Management Review, 105.
[52] T. Goban-Klas, P. Sienkiewicz, *Społeczeństwo informacyjne: szanse, zagrożenia, wyzwania*, Kraków, 1999 r, s. 139–157.

- warunki ułatwiające przechowywanie, zachowanie i rozwoju społeczeństwa informacyjnego.

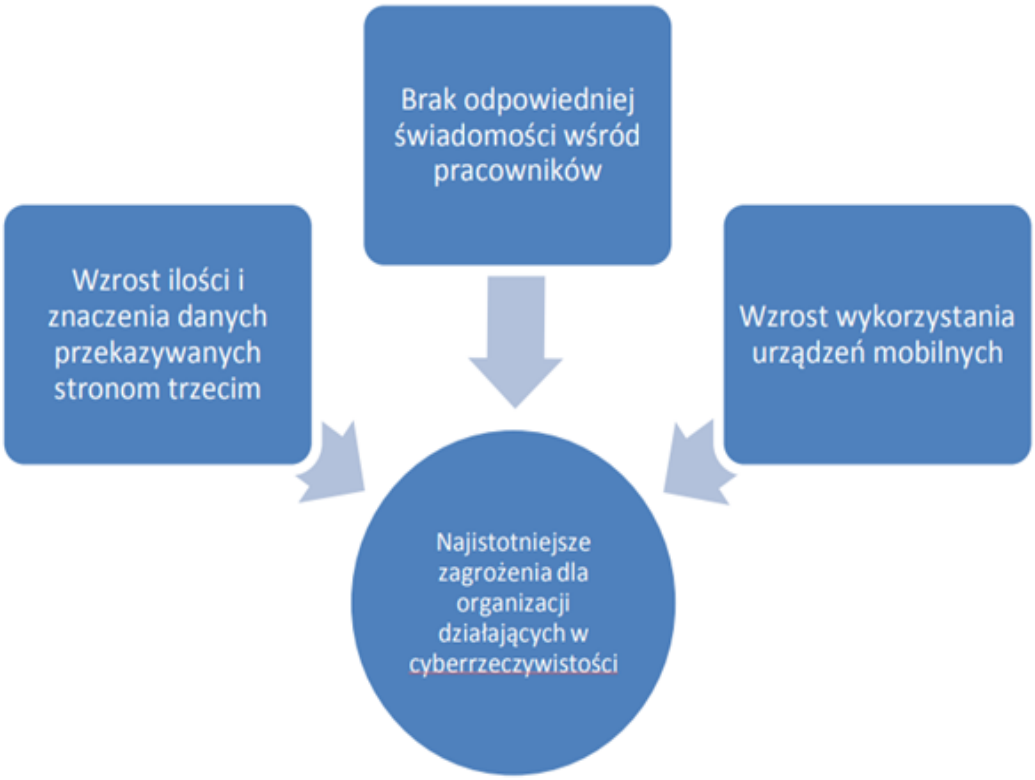
Bezpieczeństwo informacji można rozumieć jako wypadkową bezpieczeństwa prawnego, fizycznego, teleinformatycznego i osobowo-organizacyjnego[53].

Postępowanie zabezpieczające wszczynane podczas sytuacji zagrażającej systemowi lub zasobom informacyjnym są problemem trudnym i bardzo kosztownym. Dlatego istniej bardzo duży opór wśród decydentów danej instytucji, co prowadzi do tego, że są one często przerywane lub w ogóle nie stosowane. We współczesnym świece napotyka się coraz więcej zagrożeń, prowadzących do naruszania ochrony procesów gromadzenia i wykorzystania danych oraz utraty informacji. W związku ze zwiększającym się ryzykiem w tym zakresie koniecznym staje się stworzenie strategii i procedur zarządzania informacjami i ich bezpieczeństwa w danej instytucji. Taka modelowa strategia bezpieczeństwa informacyjnego powinna obejmować między innymi: systemy, procesy, osoby oraz przetwarzaną informację[54].

Do podstawowych czynników związanych z zagrożeniami bezpieczeństwa informacji zaliczyć należy:

- błędy i pomyłki człowieka – są to sytuacje takie jak niedbalstwo, brak wiedzy lub nieuwaga administratorów, projektantów, a przede wszystkim użytkowników systemu;
- awarie – nieoczekiwane uszkodzenie się i defekty sprzętu, urządzeń i oprogramowania, niezbędnych do prawidłowego przetwarzania i przechowywania zasobów;
- katastrofy– zdarzenia losowe naturalne np. powódź, trzęsienie ziemi, pożar, huragan itp. oraz wywołane przez ludzi np. katastrofy budowane, komunikacyjne, które prowadzą do zakłóceń funkcjonowania systemów;
- celowe, umyślne działania - ataki hakerskie osób włamujących się do sieci i systemów komputerowych lub zautomatyzowane ataki na system, kradzież sprzętu i zasobów. Do tego typu działań można zaliczyć również ataki wewnętrzne takie jak niezadowoleni lub przekupieni pracownicy oraz ataki zewnętrzne jak hakerzy, szpiedzy[55].

[53] J. Wołoszyn, P. Lula, *Informatyczne metody i środki ochrony zasobów informacyjnych przedsiębiorstwa*, w: System informacji strategicznej. Wywiad gospodarczy, s. 137.
[54] J. Czekaj, *Podstawy zarządzania*…,op.cit., s. 129.
[55] D. L. Pipking 2002*, Bezpieczeństwo informacji. Ochrona globalnego przedsiębiorstwa.* WNT, Warszawa, s. 26.



Źródło: L. Więcaszek-Kuczyńska, *Zagrożenia dla organizacji działających w cyberrzeczywistości*,

Rysunek 2-4
Zagrożenia dla organizacji działających w cyberrzeczywistości.

Podając za P. Bączkiem zagrożenie bezpieczeństwa informacyjnego ma swoje źródła w działalności człowieka lub organizacji i wyrażać się jako[56].

- nieuprawnione ujawnienie informacji tzw. wyciek lub przeciek;
- naruszenie przez władze praw obywatelskich;
- asymetria w międzynarodowej wymianie informacji;
- działalność grup świadomie manipulujących przekazem informacji;
- niekontrolowany rozwój nowoczesnych technologii bioinformatycznych;
- przestępstwa komputerowe;
- cyberterroryzm;
- walka informacyjna;
- zagrożenia asymetryczne;
- szpiegostwo.

Podobne stanowisko przedstawia A. Żebrowski i także ilustruje w swoich opracowaniach człowieka jako główne źródło zagrożeń bezpieczeństwa informacyjnego.

[56] P. Bączek, *Zagrożenia informacyjne*…, op.cit., s. 72-73.

Nakreśla on różnego rodzaju działania człowieka, który przy wykorzystaniu wielu różnych techniki włamań do systemów informacyjnych, będących cennym źródłem informacji stanowiących tajemnicę państwową lub służbową mogą prowadzić do naruszenia bezpieczeństwa informacyjnego.

Do technik tych można zaliczyć:

- zmowa kilku sprawców;
- celowe inicjowaniu awarii;
- wywoływanie fałszywych alarmów (uśpienie czujności);
- przeszukiwanie śmietników położonych w pobliżu firmy (pozyskanie pozornie nieważnych informacji);
- szantaż, korupcja;
- rozsyłanie do firm ankiet, zapytań, propozycji;
- rozkodowywanie hasła dostępu;
- atak słownikowy;
- podsłuch sieciowy;
- wirusy, robaki, konie trojańskie, oraz inne groźne aplikacje destabilizujące sprawność sytemu;
- wykorzystywanie luk w zabezpieczeniach dostępu do poczty elektronicznej i serwisu informacyjnego;
- techniki obchodzenia zabezpieczeń np. programy wykorzystujące błędy w systemach operacyjnych i oprogramowaniu użytkowym;
- kryptoanaliza zaszyfrowanych informacji;
- przechwytywanie otwartych połączeń sieciowych
- przechwytywanie otwartych połączeń sieciowych[57].

Jeżeli więc, w obszarach systemu informacyjnego może występować zjawisko niekontrolowanego przepływu informacji, należy natychmiast wdrożyć środki zaradcze w tym zakresie. Nie ma jednak wątpliwości, że w każdej jednostce niezbędne jest podejmowanie decyzji w tradycyjnie ujmowanych czterech podstawowych obszarach procesu zarządzania tj. planowanie, organizowanie, motywowanie i kontrolowanie. Dotyczy to również sfery bezpieczeństwa systemu informacyjnego. W ujęciu ideowym pozwolić to może kierowni-

[57]A. Żebrowski, W. Kwiatkowski, *Bezpieczeństwo informacji III Rzeczypospolitej*, Oficyna Wydawnicza ABRYS, Kraków 2000., s. 73.

kom jednostek organizacyjnych na większe skupienie w obszarach nieefektywnych, określanych także jako wąskie gardła, w celu poprawy efektywności i wydajności[58].

2.3 ZARZĄDZANIE BEZPIECZEŃSTWEM INFORMACYJNYM – ELEMENTY BEZPIECZEŃSTWA INFORMACYJNEGO W INSTYTYCJACH PUBLICZNYCH

Aby zapewnić wymagany poziom bezpieczeństwa informacyjnego i bezpieczeństwa informacji należy wdrożyć i stosować właściwe metody zarządzania. Efektywne i sprawne zarządzanie wymaga z kolei wdrożenia i odpowiedniego nowelizowania i przeprojektowania polityki bezpieczeństwa informacyjnego oraz polityki bezpieczeństwa informacji.

Rosnąca zawiłość i wielopłaszczyznowość uwarunkowań związanych z dynamicznym rozwojem globalnego społeczeństwa informacyjnego, w tym szczególnie skomplikowana natura wielu wyzwań i zagrożeń informacyjnych powoduje, iż racjonalnie konceptualizowana i realizowana polityka bezpieczeństwa informacyjnego państwa musi zawierać działania podejmowane samodzielnie, a także przy współpracy z innymi państwami i podmiotami pozapaństwowymi[59]. Wymaga to nie tylko zdatności do ustępstw, zawierania konsensusów i równoważenia interesów, ale także umiejętności długofalowej współpracy. Energiczny charakter przestrzeni bezpieczeństwa informacyjnego wymusza także potrzebę właściwego reagowania na zmiany w postaci umiejętnego wyznaczania i kształtowania priorytetów polityki bezpieczeństwa informacyjnego. W sytuacjach zmian o charakterze systemowym, także gotowości do głębokiego przeprojektowywania i redefiniowania tej polityki. Proces taki bez wątpienia wymaga posiadania i włączania w prace tworzenia i wdrażania polityki bezpieczeństwa informacyjnego odpowiedniego potencjału eksperckiego. Zadaniem takiego zespołu jest tworzenie merytorycznych podstaw do profilowania i przedkładania celów i podejmowania decyzji strategicznych.

Formułowanie przemyślanej i intencjonalnej do potrzeb państwa polityki bezpieczeństwa informacyjnego wymaga stosowania określonych reguł postępowania, do których możemy zaliczyć:

---

[58] Por. I.M. Pandey, Balanced Scorecard: *Myth and Reality*, Executive Summary, Vikalpa 2005/1, s. 1–3; B. Morard, A. Stancu, Ch. Jeannette, *Time evolution analysis and forecast of key performance indicatior in a Balanced Scorecard*, Global Journal of Business Research (GJBR) 2013/7/2, s. 9–27.

[59] M. Kubiak, S. Topolewski, *Bezpieczeństwo informacyjne w XXI wieku*, Uniwersytet Przyrodniczo-Humanistyczny w Siedlcach, Siedlce 2016, s 33.

- przyjęcie sposobu rozumienia i interpretacji pojęcia bezpieczeństwo informacyjne;
- określenie determinantów bezpieczeństwa informacyjnego;
- przyjęcie zestawu norm określających zakładany poziom bezpieczeństwa w sferze informacyjnej;
- ustalenie sposobów oceny bieżącego stanu bezpieczeństwa informacyjnego;
- wybór instrumentów i metod prognozowania sytuacji w dziedzinie bezpieczeństwa informacyjnego;
- określenie możliwych do zastosowania środków realizacji polityki bezpieczeństwa informacyjnego;
- ustalenie zasad kontroli skuteczności wdrażania i efektywności polityki bezpieczeństwa informacyjnego.

Dobrze rozwijające się i odnoszące sukcesy przedsiębiorstwo, czy instytucja nie mogą pozwolić sobie na utratę lub przypadkowe, niezamierzone i nieautoryzowane ujawnienia poufnych danych. Dlatego niezwykle ważnym działaniem podejmowanym przez firmy oraz instytucje publiczne staje się zabezpieczanie środków przechowywania danych lub przetwarzania informacji[60].

Dla ochrony polityki bezpieczeństwa informacji obowiązują akty prawne takie jak:

- Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. nr 133, poz. 883)
- Ustawa z dnia 27 lipca 2001 r. o ochronie baz danych (Dz. U. nr 128, poz. 1402)
- Ustawa z dnia 18 wrześnie 2001 r. o podpisie elektronicznym (Dz. U. nr 130, poz.1450)
- Ustawa z dnia 5 sierpni 2010 r. o ochronie informacji niejawnych (Dz. U. nr 182, poz. 1228)
- Przepisy prawa karnego znajdujące się w kodeksie karnym oraz znowelizowanych ustaw chroniących informacje, mające zastosowanie do przypadków łamania prawa przez osoby używające komputerów i sieci[61].

W szczególności polityka bezpieczeństwa powinna określać:

- zabezpieczenia fizyczne – wszystkie elementy mające na celu zabezpieczenie infrastruktury takiej jak: okna, drzwi, ściany, instalacje, montaż systemów alarmowych, czujników, telewizji przemysłowej itp.;

[60] J. Czekaj, Podstawy *zarządzania*…,op.cyt., s. 126-129.
[61] Ibidem, s. 126-129.

- zabezpieczenia wykorzystujące metody i środki informatyki – do których zaliczyć należy rozwiązania sprzętowe oraz programowe;
- zabezpieczenia organizacyjne - polegające na wprowadzeniu zmian organizacyjnych w danej instytucji, prowadzących do zwiększenie poziomu bezpieczeństwa systemu. Mowa tu o takich czynnościach jak zaprojektowanie regulaminów i procedur pracy, wprowadzenie procedury metodyki postępowania awaryjnego, obowiązków i odpowiedzialność pracowników);
- zabezpieczenia administracyjne – sekwencja prowadząca do wdrożenia wszystkich systemów certyfikacji potwierdzających przydatność do pracy w warunkach danej organizacji. Certyfikaty te mogą dotyczyć zarówno ludzi, wyposażenia, sprzętu, technologii, oprogramowania),
- rozwiązania prawne - uregulowania w prawie karnym stojące na straży bezpieczeństwa informacji dotyczące przede wszystkim poufności informacji, oszustw, manipulacji, wandalizmu, itp.[62].

Sprawowanie kontroli i zarządzanie bezpieczeństwem informacji w danej instytucji opiera się na wszystkim tym co możemy rozumieć jako elementy bezpieczeństwa informacji. Kluczowym celem tego procesu jest zarządzanie ryzykiem, co pozwala na minimalizowanie ryzyka wystąpienia zagrożeń.

Podstawowymi pojęciami, które wyjaśnia norma poświęcona technice informacyjnej, są:

- zagrożenie – sytuacja bądź stan wywołane działaniem niepożądanym - incydentem, którego skutkiem może być szkoda na rzecz systemu lub instytucji;
- zasoby – posiadanie, nagromadzenie wszystkich informacji potrzebnych i mających wartość dla instytucji,
- zabezpieczenie – procedura redukująca ryzyko
- podatność – zasób lub grupa zasobów, która może w łatwy sposób ulec zagrożeniu[63].

Zwyczajowo polityka bezpieczeństwa systemu informacyjnego powinna być kreowana przez kierownictwo jednostki organizacyjnej, w której ma być stosowana, przy wsparciu osób odpowiedzialnych za ochronę informacji znajdujących się w gestii tej jednostki.

Powinna obejmować takie elementy, jak:

- politykę informacyjną,

[62] J. Wołoszyn, P. Lula, *Informatyczne metody…,* op.cit*.,* str. 224.
[63] J. Łuczak, M. Tyburski, *Systemowe zarządzanie bezpieczeństwem informacji ISO/IEC 27001*, Uniwersytet Ekonomiczny w Poznaniu 2010. s. 20.

- ochronę informacji niejawnych,
- zasady ochrony danych osobowych,
- politykę bezpieczeństwa systemu teleinformatycznego,
- zasady ochrony tajemnicy oraz innych tajemnic zawodowych,
- zapobieganie przestępstwom na szkodę firmy, szczególnie fałszerstwom i oszustom,
- zasady ochrony fizycznej i technicznej,
- i inne związane z bezpieczeństwem[64].

Dzięki wdrożonym środkom ochronny i systemowi zarządzania bezpieczeństwem informacji kierownictwo instytucji jest w stanie zapewnić:

- realizację przyjętej misji danego podmiotu;
- dobrą markę organizacji wśród innych jednostek szkolnych;
- ciągłość pracy w organizacji;
- realizację przepisów prawnych, na przykład w ochronie tajemnicy państwowej lub danych osobowych;
- zagwarantowanie niezawodności procesów w aspekcie terminowości, dostępności informacji, dokładności, integralności informacji i ich poufności[65].

Kierownik jednostki organizacyjnej odpowiada i kieruje całością prac związanych z przetwarzaniem, zasilaniem, udostępnianiem i archiwizowaniem informacji zawartych w bazie danych, a także jest odpowiedzialny za szkolenia pracowników w zakresie metod ochrony danych, jak również szkolenia związane z pojawieniem się nowych zdarzeń będących zagrożeniem dla organizacji.

Użytkownicy systemu informacyjnego muszą być na bieżąco informowani o zasobach informacyjnych przedsiębiorstwa, tak aby mogli być przygotowani do roli aktywnego użytkownika informacji. To właśnie systemy informacyjne muszą być tak zaprojektowane i przygotowane, aby wychodzić naprzeciwko oczekiwaniom użytkowników. Powinny one przedstawiać zasoby informacyjne w ten sposób, aby zachęcić zarówno kierowników jak i pracowników do aktywnego korzystania z dostępnych źródeł informacji Aby te wzajemne relacje system informacyjny-użytkownicy zaistniały w sposób właściwy, niezbędna jest działalność szkoleniowa.

---

[64] J. Wójcik, *Kryminologiczne i kryminalistyczne problemy funkcjonowania wywiadu gospodarczego* (w:) *System informacji strategicznej,* pod red. R. Borowieckiego i M. Romanowskiej, Difin, Warszawa 2001, s. 352-353.

[65] K. Liderman, Bezpieczeństwo *informacyjne*…,*op.cit*.,s. 158.

Działania przedsiębiorstwa związane ze szkoleniem użytkowników informacji powinny być dostosowane do różnego poziomu i rodzaju odbiorców ze znacznym naciskiem na naukę wyszukiwana informacji[66].

Istotne elementy umiejętnego korzystania z zasobów przez użytkowników obejmują:

- fachowe i kompetentne rozpoznanie własnych potrzeb,
- eksplorowanie właściwej informacji spośród wielu innych,
- wartościowanie relewantności wygenerowanych informacji oraz sposobu ich organizacji i przechowywania,
- produktywne i skuteczne zastosowanie zgromadzonych danych.

Przedsiębiorstwo powinno zapewnić jak najlepszą i jak najszybszą obsługę systemu informacyjnego dla użytkowników, poprzez udostępnianie[67]:

- katalogów i własnych baz danych,
- katalogów i baz danych innych podmiotów poprzez sieci komputerowe
- informacji w rozległych sieciach komputerowych,
- komercyjnych baz za pośrednictwem sieciowego systemu baz danych.

Należy podkreślić, że z pewnego punktu widzenia system zautomatyzowany jest zawsze w jakimś stopniu niedogodny. Posługiwanie się nim oznacza dla jego odbiorcy działanie w środowisku sztucznym, niepewnym, często nieprzewidywalnym.
Natomiast uczynienie systemu przyjaznym użytkownikowi stanowi problem, który ma wiele poprawnych rozwiązań. Stosowane dotychczas rozwiązania zmierzają w dwóch kierunkach. Pierwszy to koncepcja polegającą na "oswajaniu" użytkownika ze sztucznym środowiskiem poprzez stosowanie różnorodnych udogodnień i ułatwień o rozbudowaną pomoc - jest to podejście systemocentryczne. W drugiej grupie znajdują się pomysły wprowadzania takich sposobów realizowania relacji użytkownika informacji z systemem informacyjnym, które naśladowałyby użytkownika w naturalnym dla niego środowisku, podtrzymywałyby i utwierdzałyby jego nawyki, preferencje oraz postawy - jest to podejście „użytkownikocentryczne”[68].

Na podstawie wnikliwej analizy stanu prawnego i uwarunkowań organizacyjnych, zgodnie z art. 13 ust. 1 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne, podmiot publiczny używa do realizacji zadań

[66] M. Próchnicka, *Informacja a umysł*, PWN, Kraków 1991 rok, s.50.
[67] J. Kisielnicki, H. Sroka, *Systemy informacyjne biznesu, Agencja wydawnicza,* "Placet", Warszawa 1999 rok., s. 15.
[68] M. Próchnicka, *Informacja*…, op.cit., s.51.

publicznych systemów teleinformatycznych spełniających minimalne wymagania dla systemów teleinformatycznych oraz zapewniających interoperacyjność systemów na zasadach określonych w Krajowych Ramach Interoperacyjności.

W myśl § 15 ust. 1 rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych, systemy teleinformatyczne używane przez podmioty realizujące zadania publiczne projektuje się, wdraża oraz eksploatuje przy zastosowaniu norm oraz uznanych w obrocie profesjonalnym standardów i metodyk, z uwzględnieniem ich:

- funkcjonalności,
- niezawodności,
- używalności,
- wydajności,
- przenoszalności
- pielęgnowalności.

Zarządzanie usługami realizowanymi przez systemy teleinformatyczne ma na celu dostarczanie tych usług na deklarowanym poziomie dostępności i odbywa się w oparciu o udokumentowane procedury. Wymagania te uznaje się za spełnione, jeśli projektowanie, wdrażanie, eksploatowanie, monitorowanie, przeglądanie, utrzymanie i udoskonalanie zarządzania usługą podmiotu realizującego zadanie publiczne odbywają się z uwzględnieniem Polskich Norm: PN-ISO/IEC 20000-1 i PN-ISO/IEC 20000-2.

System teleinformatyczny używany do realizacji zadań publicznych musi obsługiwać standardy zapewniające dostęp do zasobów informacji oraz formaty danych określone w jego załączniku. Podmiot realizujący zadania publiczne opracowuje i ustanawia, wdraża i eksploatuje, a także monitoruje i przegląda oraz utrzymuje i doskonali system zarządzania bezpieczeństwem informacji.

System ten powinien zapewniać:

- poufność,
- dostępność
- integralność informacji.

Ponadto system taki powinien uwzględniać takie atrybuty jak:[69]

- autentyczność,
- rozliczalność,
- niezaprzeczalność
- niezawodność.

Zarządzanie bezpieczeństwem informacji powinno być realizowane w szczególności poprzez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie działań w zakresie:

1) zapewnienia aktualizacji regulacji wewnętrznych w zakresie dotyczącym zmieniającego się otoczenia;

2) utrzymywania aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację;

3) przeprowadzania okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji oraz podejmowania działań minimalizujących to ryzyko, stosownie do wyników przeprowadzonej analizy;

4) podejmowania działań zapewniających, że osoby zaangażowane w proces przetwarzania informacji posiadają stosowne uprawnienia i uczestniczą w tym procesie w stopniu adekwatnym do realizowanych przez nie zadań oraz obowiązków mających na celu zapewnienie bezpieczeństwa informacji;

5) bezzwłocznej zmiany uprawnień, w przypadku zmiany zadań osób, o których mowa w pkt. 4;

6) zapewnienia szkolenia osób zaangażowanych w proces przetwarzania informacji ze szczególnym uwzględnieniem takich zagadnień, jak:

a) zagrożenia bezpieczeństwa informacji,

b) skutki naruszenia zasad bezpieczeństwa informacji, w tym odpowiedzialność prawna,

c) stosowanie środków zapewniających bezpieczeństwo informacji, w tym urządzenia i oprogramowanie minimalizujące ryzyko błędów ludzkich;

7) zapewnienia ochrony przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami, przez:

a) monitorowanie dostępu do informacji,

[69] § 20 ust. 1 rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych.

b) czynności zmierzające do wykrycia nieautoryzowanych działań związanych z przetwarzaniem informacji,

c) zapewnienie środków uniemożliwiających nieautoryzowany dostęp na poziomie systemów operacyjnych, usług sieciowych i aplikacji;

8) ustanowienia podstawowych zasad gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość;

9) zabezpieczenia informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikacje, usunięcie lub zniszczenie;

10) zawierania w umowach serwisowych podpisanych ze stronami trzecimi zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji;

11) ustalenia zasad postępowania z informacjami, zapewniających minimalizację wystąpienia ryzyka kradzieży informacji i środków przetwarzania informacji, w tym urządzeń mobilnych;

12) zapewnienia odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych, polegającego w szczególności na:

a) dbałości o aktualizację oprogramowania,

b) minimalizowaniu ryzyka utraty informacji w wyniku awarii,

c) ochronie przed błędami, utratą, nieuprawnioną modyfikacją,

d) stosowaniu mechanizmów kryptograficznych w sposób adekwatny do zagrożeń lub wymogów przepisu prawa,

e) zapewnieniu bezpieczeństwa plików systemowych,

f) redukcji ryzyk wynikających z wykorzystania opublikowanych podatności technicznych systemów teleinformatycznych,

g) niezwłocznym podejmowaniu działań po dostrzeżeniu nieujawnionych podatności systemów teleinformatycznych na możliwość naruszenia bezpieczeństwa,

h) kontroli zgodności systemów teleinformatycznych z odpowiednimi normami i politykami bezpieczeństwa;

13) bezzwłocznego zgłaszania incydentów naruszenia bezpieczeństwa informacji w określony i z góry ustalony sposób, umożliwiający szybkie podjęcie działań korygujących;

14) zapewnienia okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji, nie rzadziej niż raz na rok.

Obowiązki, o których mowa powyżej uznaje się za spełnione, jeżeli system zarządzania bezpieczeństwem informacji został opracowany na podstawie Polskiej Normy PN-ISO/IEC 27001, a ustanawianie zabezpieczeń, zarządzanie ryzykiem oraz audytowanie odbywa się na podstawie Polskich Norm związanych z tą normą, w tym:

- PN-ISO/IEC 27002 – w odniesieniu do ustanawiania zabezpieczeń;
- PN-ISO/IEC 27005 – w odniesieniu do zarządzania ryzykiem;
- PN-ISO/IEC 24762 – w odniesieniu do odtwarzania techniki informatycznej po katastrofie w ramach zarządzania ciągłością działania.

Od 25 maja 2018 r. zaczęło obowiązywać unijne ogólne rozporządzenie o ochronie danych (RODO). Wskazuje ono podstawowe zasady ochrony danych osobowych, wśród których można wyróżnić następujące zasady:

- przetwarzania zgodnego z prawem, rzetelnego i przejrzystego,
- ograniczenia celu zbierania danych,
- minimalizacji danych,
- ograniczenia celu przetwarzania danych,
- prawidłowości przetwarzania danych,
- integralności i poufności przetwarzania,
- rozliczalności przetwarzania.

W art. 24 RODO określone zostały obowiązki administratora, gdzie uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia, administrator wdraża odpowiednie środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z niniejszym rozporządzeniem. Środki te są w razie potrzeby powinny być poddawane przeglądom i uaktualniane. Jeżeli jest to proporcjonalne w stosunku do czynności przetwarzania, środki te, obejmują wdrożenie przez administratora odpowiednich polityk ochrony danych.

W preambule do RODO określono, iż przetwarzanie danych osobowych w zakresie bezwzględnie niezbędnym i proporcjonalnym do zapewnienia bezpieczeństwa sieci i informacji, czyli:

- zapewnienia odporności sieci lub systemu informacyjnego na danym poziomie poufności na przypadkowe zdarzenia albo niezgodne z prawem lub nieprzyjazne działania naruszające dostępność, autentyczność, integralność i poufność przechowywanych lub przesyłanych danych osobowych

- bezpieczeństwa związanych z nimi usług oferowanych lub udostępnianych poprzez te sieci i systemy przez organy publiczne, zespoły reagowania na zagrożenia komputerowe, zespoły reagowania na komputerowe incydenty naruszające bezpieczeństwo, dostawców sieci i usług łączności elektronicznej oraz dostawców technologii i usług w zakresie bezpieczeństwa jest prawnie uzasadnionym interesem administratora, którego sprawa dotyczy.

Może to obejmować na przykład:

- zapobieganie nieuprawnionemu dostępowi do sieci łączności i rozprowadzaniu złośliwych kodów,
- przerywanie ataków typu „odmowa usługi"
- przeciwdziałanie uszkodzeniu systemów komputerowych i systemów łączności elektronicznej.

Zgodnie natomiast z art. 30 ust. 1 RODO, każdy administrator jest zobowiązany do prowadzenia rejestru czynności przetwarzania danych osobowych, za które odpowiada. W rejestrze tym zamieszcza się wszystkie informacje wyszczególnione w tym przepisie. Również podmiot, któremu powierzono przetwarzanie danych osobowych, zobowiązany jest do prowadzenia rejestru wszystkich kategorii czynności przetwarzania dokonywanych w imieniu administratora.

Rejestry te mają formę pisemną, w ramach której ustawodawca unijny przewiduje również formę elektroniczną. Rejestr podlega obowiązkowi udostępnienia na żądanie organu nadzorczego. Ponadto RODO wskazuje, że dla zachowania zgodności z niniejszym rozporządzeniem, administrator lub podmiot przetwarzający powinni prowadzić rejestry czynności przetwarzania, za które są odpowiedzialni. Każdy administrator i każdy podmiot przetwarzający powinni mieć obowiązek współpracować z organem nadzorczym i na jego żądanie udostępniać mu te rejestry w celu monitorowania tych operacji przetwarzania.

W celu zachowania bezpieczeństwa i zapobiegania przetwarzaniu niezgodnemu z niniejszym rozporządzeniem administrator lub podmiot przetwarzający powinni oszacować ryzyko właściwe dla przetwarzania. Ponadto powinni wdrożyć środki takie jak szyfrowanie minimalizujące to ryzyko. Środki takie powinny zapewnić odpowiedni poziom bezpieczeństwa, w tym poufność oraz uwzględniać stan wiedzy technicznej oraz koszty ich wdrożenia w stosunku do ryzyka i charakteru danych osobowych podlegających ochronie.

Oceniając ryzyko w zakresie bezpieczeństwa danych, należy wziąć pod uwagę ryzyko związane z przetwarzaniem danych osobowych takie jak przypadkowe lub niezgodne z prawem zniszczenie, utracenie, zmodyfikowanie, nieuprawnione ujawnienie lub nieu-

prawniony dostęp do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych i mogące w szczególności prowadzić do uszczerbku fizycznego, szkód majątkowych lub niemajątkowych.

Bezpieczeństwo przetwarzania danych osobowych zostało uregulowane w art. 32 RODO, który mówi, że uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia, administrator i podmiot przetwarzający mają obowiązek wdrożyć odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku, w tym między innymi w stosownym przypadku:

a) pseudonimizację i szyfrowanie danych osobowych;

b) zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania;

c) zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego;

d) regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.

Oceniając, czy stopień bezpieczeństwa jest odpowiedni, uwzględnia się w szczególności ryzyko wiążące się z przetwarzaniem, w szczególności wynikające z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych. Zgodnie z art. 32 ust. 3 RODO, wywiązywanie się przez administratora i podmiot przetwarzający z obowiązków, o których mowa powyżej, można wykazać między innymi poprzez stosowanie zatwierdzonego kodeksu postępowania lub zatwierdzonego mechanizmu certyfikacji. Zgodnie z art. 37 ust. 1 lit. a RODO, w przypadku, gdy przetwarzania dokonują organ lub podmiot publiczny, administrator i podmiot przetwarzający wyznaczają zawsze inspektora ochrony danych. Zadania inspektora ochrony danych określa art. 39 RODO. Zgodnie z art. 38 ust. 6 RODO inspektor ochrony danych może wykonywać inne obowiązki, jednak najwyższe kierownictwo zapewnia by takie zadania i obowiązki nie powodowały konfliktu interesów.

WNIOSKI

Informacja od zawsze była i zawsze będzie jedną z najważniejszych wartości dla każdego człowieka, społeczeństwa, gospodarki, państwa czy instytucji. Informacja jest zasobem, która w dzisiejszych czasach jest najczęściej poszukiwany[70]. Odkąd pojawił się internet oraz telefonia komórkowa, odległość przy wymianie informacji przestała mieć jakiekolwiek znaczenie. Uprościło nam to również poszukiwanie informacji, mamy do niej o wiele lepszy dostęp niż kiedyś. Informacja odzwierciedla realia panujące w życiu społecznym[71].

Dzisiejszy świat wymaga korzystania z wielu informacji. Ludzie włączeni są w różnorodne procesy społeczne, polityczne, gospodarcze, ekonomiczne, są zalewani różnymi informacjami. Dlatego też państwo czy społeczeństwo bez rzeczowo ukształtowanej sfery informacyjnej nie może skutecznie funkcjonować. Eksplozja Internetu zmieniła wszystko: relacje między ludźmi, sposób uprawiania polityki, działanie firm i mechanizmy osiągania sukcesu. Kto jest dobrze poinformowany, ten trafnie decyduje. Informacja jest czymś tak cennym jak bogactwo naturalne: węgiel, ropa czy gaz. Społeczeństwo XXI wieku to społeczeństwo szerokiego obiegu informacji. Zatem XXI wiek opiera się na informacji oraz na środkach jej przetwarzania i przesyłania. Społeczeństwo informacyjne XXI wieku określane jest często, jako społeczeństwo „ryzyka" albo „zmediatyzowane", chociaż według innych zmienia się w społeczeństwo „wiedzy i refleksji", a nawet „mądrości". Pierwsze dwa określenia odzwierciedlają nastroje lęku i obaw, z kolei dwa następne rodzą nadzieję na zwiększenie zasobów wiedzy i rozwagę, co może się przyczynić do wzrostu mądrości w jego funkcjonowaniu. Wnioski płynące z analizy wieku informacji mogą być różne, w zależności od przyjęcia optymistycznego lub pesymistycznego scenariusza jego rozwoju. Jak zwykle stosowne jest zachowanie umiaru i rozsądku w formowaniu ocen. Dostrzega się jednak przewagę szans rozwojowych nad zagrożeniami. Rzecz w tym, aby umieć wykorzystać szanse oraz zabezpieczyć się przed wykrytymi w porę zagrożeniami.

Postępujący rozwój informatyzacji wraz z uzależnieniem większości aspektów działalności człowieka od systemów informatycznych sprawi, iż powiększy się katalog zagrożeń bezpieczeństwa informacyjnego. Sprawia to, że wiele krajów oraz organizacji rządowych podejmuje działania zawierające elementy współczesnej walki informacyjnej oraz odwrotnie próbuje się przed nią zabezpieczyć. Sprawia to, że tematyka niniejszej dysertacji jest bardzo aktualnym i ciekawym tematem rozważań.

[70] J. Łuczak, M. Trybulski, *Systemowe ...,* op.cit., s. 7.
[71] W. Krztoń, *XXI wiek...,* op.cit., s 101.

Należy zatem zgodzić się z J. Łuczakiem, iż niewiele sytuacji kryzysowych firmy można porównać z utratą informacji, szczególnie, że jak dowodzi praktyka, utrata informacji to incydenty coraz bardziej powszechne i trudne do wykrycia, przynoszące konsekwencje prawne, finansowe, utratę wiarygodności podmiotu dopuszczającego do nieuprawnionego dostępu osób trzecich do swoich danych, a obserwowany we współczesnej rzeczywistości gospodarczej dynamiczny rozwój sieci komputerowych przyczynia się także do tego, iż zbiory danych przepływają między organizacjami w sposób nie zawsze należycie kontrolowany, zaś komputerowe przetwarzanie danych umożliwia centralizację przechowywania i przetwarzania zasobów informacyjnych, co powoduje niespotykane dotąd zagrożenie utraty zasobów informacyjnych[72].

Rozważając zagrożenia bezpieczeństwa informacyjnego należy także zaznaczyć, iż pewne informacje, stanowią w organizacji wiadomości chronione, a tajność to jeden z atrybutów ochrony informacji (obok m.in. integralności, dostępności, niezaprzeczalności i autentyczności) stanowiący o wymaganym stopniu ochrony informacji przed nieuprawnionym dostępem.

Analiza literatury przedmiotu oraz wieloletnia praktyka autora niniejszej dysertacji przy obserwacji użytkowników systemów teleinformatycznych pozwalają stwierdzić, iż utrata danych może nastąpić nie tylko z przyczyn losowych (obiektywnych), takich jak uszkodzenie sprzętu teleinformatycznego, czy błędy użytkownika, ale przede wszystkim na skutek zamierzonego działania osób, które celowo chcą uzyskać nieuprawniony dostęp do zasobów, aby nielegalnie zawładnąć zgromadzonymi lub dystrybuowanymi danymi. Człowiek jest zaś najsłabszym ogniwem bezpieczeństwa, gdyż urządzenia techniczne, oprogramowanie to jedynie narzędzia obsługiwane przez ludzi i przede wszystkim od użytkownika będzie zależało utrzymanie informacji z dala od dostępu osób nieuprawnionych.

Dokonując analizy znaczenia informacji stwierdzić należy, że odgrywa ona niezwykle istotną rolę w funkcjonowaniu organizacji zhierarchizowanej jaką jest Państwowa Straż Pożarna. Najważniejszym zadaniem informacji jest przekazanie odpowiednich danych przy wykorzystaniu systemu informacyjnego. Informacja transportowana jest od nadawcy do odbiorcy za pomocą kanałów informacyjnych, a jej zadaniem jest zmniejszenie luki informacyjnej, polegające na dostarczeniu odbiorcy określonej wiedzy. Istotną rolę w tym procesie odgrywa odbiorca, dla którego informacja jest przeznaczona, bowiem od

[72] M. Wrzosek*, Procesy informacyjne…,* op.cyt., s.153.

jego umiejętności zrozumienia przekazywanych treści i poprawności ich interpretacji zależy skuteczność i efektywność komunikacji.

Gwałtowny postęp cywilizacyjny, powstanie zbiorów olbrzymich zasobów informacji oraz rozwój środków komunikowania jako zjawiska charakterystyczne dla czasów nam współczesnych, niosą szczególne zagrożenia dla bezpieczeństwa informacyjnego, a katalog tych zagrożeń jest katalogiem otwartym, gdyż wraz z rozwojem społeczeństwa informacyjnego pojawiają się nowe możliwości i wyzwania. Zagrożenia bezpieczeństwa informacyjnego są definiowane w różnorakich obszarach ryzyka, szczególnie wyraźnie w obszarze zagrożeń technologicznych jako następstwo rozwoju technologicznego. Jednak choć to systemy informatyczne przetwarzają dane, człowiek bogaty w wiedzę, ale przecież niedoskonały, stwarza potencjalne zagrożenie dla bezpieczeństwa informacyjnego. Umiejscowienie zagrożenia, w tym zagrożenia informacyjnego, w sferze świadomości podmiotu skłania do postawienia pytań o stopień odbierania pewnych zjawisk przez ten podmiot i o określenie, czy wszystkie zjawiska zagrażające bezpieczeństwu informacyjnemu istotnie są zagrożeniem, czy może jedynie biznesowym wyzwaniem. Nie podlega wątpliwości, że zagrożenia bezpieczeństwa informacyjnego są zjawiskami realnymi, obecnymi w codziennej rzeczywistości naszego życia, zatem rozpoznanie, osiągnięcie, utrzymanie i doskonalenie bezpieczeństwa informacyjnego staje się nieodzowne do zapewnienia przewagi konkurencyjnej organizacji, płynności finansowej, rentowności, a także pozostawania w zgodzie z literą prawa.

Analiza literatury w przedmiotowym obszarze pozwala założyć hipotezę, że każda informacja podczas procesu jej przekazywania ulega zniekształceniom w kanale informacyjnym. Aby zminimalizować te zniekształcenia, potrzebne jest podejmowanie wszelkich możliwych działań, aby zapewnić przekazywanie informacji o treści tożsamej lub jak najbardziej zbliżonej do informacji pierwotnej. Najczęściej zniekształcenia powodowane są przez szum informacyjny, na który składa się nadmiar informacji docierających do odbiorcy. Do kolejnych elementów najczęściej zakłócających przepływ informacji można zaliczyć chaotyczność, niespójność oraz nieaktualność informacji. Sposobem do minimalizowania szumów informacyjnych pojawiających się w organizacji jest bieżąca selekcja informacji. Ponadto istotne jest utworzenie stanowiska pracy, w którego zakres obowiązków wchodziłoby zbieranie, selekcjonowanie i przygotowywanie, a następnie przekazywanie informacji do określonych grup odbiorców.

Struktura organizacyjna Państwowej Straży Pożarnej oraz specyficzne rodzaje wię-

zi w organizacji zhierarchizowanej powodują, że droga przepływu informacji jest znacznie dłuższa, a informacja bardziej narażona jest na zniekształcenia. Zapewniając rzetelność, aktualność i kompletność informacji kierownictwo organizacji ma kluczowy wpływ na jej funkcjonowanie oraz podnosi sprawność i skuteczność podejmowania racjonalnych i trafnych decyzji. Konieczne jest także wdrożenie właściwego systemu szkoleń dla funkcjonariuszy i pracowników PSP, bo to podniesie znacząco poziom wykonywanych przez nich zadań stawianych przed tą formacją. Zatem konieczne jest stworzenie oferty edukacyjnej, która dostosowana będzie do potrzeb oraz oczekiwań zarówno instytucji jak i samych członków organizacji. Można to osiągnąć poprzez weryfikowanie istniejących programów szkoleń pod względem ich przydatności, a także opracowywanie i wdrażanie nowych programów szkoleniowych.

Z przeprowadzonych obserwacji autora dysertacji wynika, że za słabe strony systemu szkolenia w Państwowej Straży Pożarnej można uznać:

- brak powiązań szkoleń ze ścieżką rozwoju zawodowego;
- brak obligatoryjności szkoleń specjalistycznych;
- brak możliwości zaspokojenia potrzeb szkoleniowych; niski potencjał szkoleniowy ośrodków szkolenia.

Z analizy literatury oraz przeprowadzonych obserwacji jednoznacznie wynika, że największym zagrożeniem dla bezpieczeństwa systemu informacyjnego i samej informacji jest człowiek. Zagrożenia najczęściej wynikają z niedbalstwa, braku wiedzy lub nieuwagi użytkowników systemów. Działania człowieka mogą przybrać także formę rozmyślną, polegającą na celowych atakach na systemy. Do negatywnych postępowań należy zaliczyć także kradzieże sprzętu i zasobów, czy też szpiegowanie lub hakowania.

Biorąc pod uwagę powyższe konieczne wydaje się prowadzenie systematycznych szkoleń w organizacji tak aby pracownicy mieli dostęp do wiedzy o istniejących zagrożeniach i możliwych postaciach ich występowania.

Rozdział 3 ZAGROŻENIA BEZPIECZEŃSTWA SYSTEMU INFORMACYJNEGO NA PRZYKŁADZIE PAŃSTWOWEJ STRAŻY POŻARNEJ.

Informacja to podstawowy element determinujący sukces każdej organizacji. Jest ona jednym z jego najistotniejszych zasobów. Każdy pracownik instytucji powinien ją więc należycie chronić. Co za tym idzie bardzo istotna jest odpowiednia ochrona informacji, która powinna spełniać należyty stopień bezpieczeństwa informacji. Aby to osiągnąć należy w odpowiedni sposób przygotować zasoby osobowe, organizacyjne i techniczne organizacji, a następnie w odpowiedni sposób nimi zarządzać. Należy więc właściwie ułożyć, a następnie egzekwować politykę bezpieczeństwa informacji[1].

Każda organizacja, w szczególności instytucje publiczne, są w posiadaniu informacji, które muszą być chronione czy to ze względu prawnego (np. informacje niejawne, dane osobowe) czy ze względu na interes danej organizacji (np. informacje inwestycyjne, finansowe, patenty itp.).

Ciągle zwiększający się w życiu codziennym obywateli udział technologii informatycznych oraz oczekiwania społeczne do coraz szybszego i łatwiejszego załatwienia spraw urzędowych i nie tylko powodują, że instytucje publiczne w tym Państwowa Straż Pożarna wykorzystują to w coraz większym i szerszym stopniu i zakresie technologie informatyczne. Społeczeństwo oczekuje nie tylko udogodnień i ułatwień w zakresie funkcjonowania e-administracji, ale także gwarancji, że wszelkie udostępnione przez nich dane, które wejdą w posiadanie przez administrację publiczną są adekwatnie zabezpieczone przed dostępem osób nieuprawnionych.

Bezustannie wzrasta zainteresowanie obywateli elektroniczną formą załatwiania spraw urzędowych, ale również same urzędy i instytucje administracji publicznej w coraz to większym stopniu w celu załatwienia swoich spraw komunikują się wzajemnie za pośrednictwem środków komunikacji elektronicznej. Wobec tego zapewnienie bezpieczeństwa przetwarzania informacji w Państwowej Straży Pożarnej staje się jednym z najistotniejszych i największych wyzwań stojących przed administracją publiczną.

Niewłaściwe zarządzanie bezpieczeństwem informacji może doprowadzić do niepożądanego wycieku, utraty bądź sfałszowania posiadanych danych. Mogą wystąpić także

[1] M. Kowalewski, A. Ołtarzewska, *Polityka bezpieczeństwa informacji instytucji na przykładzie Instytutu Łączności - Państwowego Instytutu Badawczego*, nr 3-4, 2007 r., s. 4.

takie zagrożenia, które zdołają doprowadzić do całkowitego paraliżu pracy instytucji, czy urzędu. Zgodnie z rozporządzeniem Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych to podmiot realizujący zadania publiczne opracowuje, ustanawia, wdraża i eksploatuje, a także monitoruje i przegląda oraz utrzymuje i doskonali system zarządzania bezpieczeństwem informacji. Ponadto system ten powinien zapewnić poufność, dostępność i integralność informacji[2].

Wymagania w zakresie zapewnienia ochrony danych osobowych zostały określone w nowym unijnym rozporządzeniu RODO, które weszło w życie w dniu 25 maja 2018 r. Tym samym przepisy dotyczące ochrony danych osobowych dla wszystkich państw członkowskich zostały ujednolicone. Celem RODO jest między innymi usprawnienie i ulepszenie przepisów i norm z zakresu ochrony danych osobowych oraz ich uporządkowanie. Wcześniejsze przepisy, które obowiązywały od 1995 r. w dobie szybko postępującej cyfryzacji miały coraz mniejsze zastosowanie praktyczne i odstawały od obecnych realiów. Zarazem RODO zostało zaadiustowane w taki sposób, aby było zawsze aktualne i uwzględniało dalszy rozwoju technologii.

Ochrona systemu bezpieczeństwa informacji wymaga zaprojektowania w Państwowej Straży Pożarnej całego systemu tej ochrony, w tym ustanowienia procedur i norm dla wszystkich procesów zachodzących w instytucji, uwzględniając przy tym wszystkie procesy wykorzystania danych osobowych. Należy wdrożyć takie rozwiązania w celu sprawniejszej komunikacji w sytuacjach kryzysowych i koordynacji bieżących działań na terenie kraju oraz w międzynarodowych akcjach ratowniczych.

W wyniku własnych doświadczeń autora niniejszej dysertacji, ale także wnikliwej analizy dokumentów źródłowych odnośnie do wdrażania wybranych wymagań dotyczących systemów teleinformatycznych, czy też wymiany informacji w postaci elektronicznej można dopatrzeć się wielu nieprawidłowości w tym obszarze. Na ogół w instytucjach publicznych w niedostateczny sposób przywiązywana jest odpowiednia waga do zapewnienia bezpieczeństwa przetwarzania informacji przy wykorzystaniu zaprojektowanego systemu. Dotyczy to między innymi braku opracowania i wdrożenia polityk bezpieczeństwa infor-

[2] Rozporządzeniem Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych Dz. U. z 2017 r. poz. 2247.

macji, blokowania lub odbierania dostępu do systemu byłym pracownikom, nie przeprowadzania obowiązkowego audytu bezpieczeństwa informacji.

Podjęte w tym rozdziale rozważania miały na celu przedstawienie stawianego w niniejszej dysertacji celu poznawczego, który został zdefiniowany jako *identyfikacja zagrożeń i możliwych usprawnień w systemie bezpieczeństwa informacji w Państwowej Straży Pożarnej jako organizacji publicznej*, w kontekście rozwiązania szczegółowego problemu badawczego wyrażonego w pytaniu: *Jak funkcjonuje system bezpieczeństwa wymiany informacji w organizacji publicznej jaką jest Państwowa Straż Pożarna?*

W celu udzielenia odpowiedzi na problem badawczy, na podstawie istniejących informacji, zweryfikowano przyjętą hipotezę, która stanowi przypuszczenie, że *Państwowa Straż Pożarna jako instytucja odpowiedzialna za zapewnienie bezpieczeństwa obywatelom naszego Państwa gromadzi i przetwarza tylko niezbędna informacje w tym zakresie. Informacje te uzyskiwane są od „klientów" i instytucji, z którymi straż pożarna współpracuje. Informacje te przechowywane są w systemach informatycznych, dlatego bardzo ważne jest by prawidłowo funkcjonował system bezpieczeństwa wymiany informacji i każdy z pracowników tej instytucji powinien ją należycie chronić. Przypuszcza się natomiast, że jednym z najważniejszych potencjalnych źródeł zagrożeń dla bezpieczeństwa informacji w danej organizacji jest naruszanie przepisów chroniących te organizacje przez osoby, które posiadają dostęp do informacji. Występują zagrożenia w bezpieczeństwie sytemu informacyjnego dlatego, że dotychczasowe zabezpieczania informacji i procedury bezpieczeństwa informacyjnego nie są przez wszystkich użytkowników w należyty sposób przestrzegane. Do tego, występuje brak świadomości wśród niektórych użytkowników o skutkach łamania zasad korzystania z systemu informacyjnego i braku odpowiedzialności. Napotyka się również bariery oraz trudności powiązane bezpośrednio z wdrażaniem w życie ustawy o ochronie informacji niejawnych.*

Ponadto zakłada się, że jako typowe zagrożenia systemu bezpieczeństwa obiegu informacji można wyodrębnić zagrożenia wewnętrzne i zewnętrzne powstające poza organizacją, w wyniku celowego lub przypadkowego działania ze strony osób trzecich. Do tych pierwszych zaliczyć możemy: zagrożenie utratą, uszkodzeniem danych lub brakiem możliwości obsługi z powodu błędu jak i przypadku; zagrożenie utratą lub uszkodzeniem poprzez celowe działania nieuczciwych użytkowników; zagrożenia fizyczne, w których szkoda jest spowodowana wypadkiem, awarią, lub innym nieprzewidzianym zdarzeniem losowym.

Do zagrożeń zewnętrznych zaliczyć możemy: przestępstwa wykorzystujące komputer jako narzędzie; cyberterroryzm; utrata informacji związana z włamaniami komputerowymi, złośliwymi kodami i wirusami, szpiegostwem, sabotażem, czy też wandalizmem.

Dla uzyskania lepszego zrozumienia zjawiska i rozwiązania problemu badawczego oraz weryfikacji sformułowanej hipotezy, przyjęto następujące metody badawcze:

1. teoretyczne:

a) analizę - stosowaną głównie w badaniu literatury przedmiotu,

b) syntezę – wykorzystywaną głównie podczas łączenia efektów analizy w syntetyczną całość,

2. empiryczne:

a) sondaż diagnostyczny badania opinii techniką ankiety z wykorzystaniem narzędzia w postaci arkusza ankiety – pozwalający na poznanie opinii respondentów na temat bezpieczeństwa systemu informacyjnego pośród funkcjonariuszy Państwowej Straży Pożarnej,

b) metodę obserwacji techniką obserwacji z wykorzystaniem narzędzia w postaci arkusza obserwacji – celem której będzie zebranie wszelkich spostrzeżeń związanych z systemem informacyjnym w Państwowej Straży Pożarnej i zagrożeń w jego funkcjonowaniu.

Naturalnie w celu zbadania tematu konieczne jest dodatkowo zastosowanie innych metod teoretycznych w postaci:

- abstrahowania – w celu wyodrębnienia lub pominięcia pewnych elementów związanych z systemem informacyjnymi jego bezpieczeństwem, które z pewnych przyczyn uznano za istotne, mające wpływ na analizowane zagadnienie oraz te, które dla tej analizy nie mają większego znaczenia,
- uogólnienia – polegające na łączeniu określonych przedmiotów analizy w oparciu o ich podobieństwa,
- wnioskowania – wypracowanie spostrzeżeń będących przedmiotem analizy bezpieczeństwa systemu informacyjnego.

3.1 PAŃSTWOWA STRAŻ POŻARNA JAKO ORGANIZACJA ZHIERARCHIZOWANA WYKORZYSTUJĄCA SYSTEMY INFORMACYJNE.

Elementem bezpieczeństwa publicznego kraju jest bezpieczeństwo przeciwpożarowe oraz bezpieczeństwo przed skutkami innych miejscowych zagrożeń. Państwowa Straż Pożarna jest jednym z podmiotów tego systemu realizującym zadania w ogólnym systemie bezpieczeństwa państwa i porządku publicznego[3].

Państwowa Straż Pożarna jest formacją składającą się z jednostek administracji publicznej, wzajemnie ze sobą powiązanych, mających możliwość wymiany doświadczeń, wiedzy oraz informacji w zakresie wykonywania ustawowych zadań walki z pożarami, klęskami żywiołowymi i innymi miejscowymi zagrożeniami, celem dążenia do ciągłego oraz zharmonizowanego rozwoju wszystkich swoich podmiotów.

Państwowa Straż Pożarna odgrywa istotną rolę w zapewnieniu bezpieczeństwa obywatelom państwa, gdyż w zakresie jej działania nie leży tylko i wyłącznie gaszenie pożarów, ale także usuwanie skutków innych miejscowych zagrożeń, ale także kontrolowanie działalności która temu bezpieczeństwu może zagrozić[4].

System wymiany informacji w Państwowej Straży Pożarnej, oprócz konieczności zapewnienia szybkiej, pewnej i sprawnej komunikacji na wielu płaszczyznach i poziomach w samej organizacji, stanowi również element Systemu Powiadamiania Ratunkowego w Polsce, będąc jego częścią, a tym częścią systemu bezpieczeństwa wewnętrznego państwa.

Ponadto system wymiany informacji w Państwowej Straży Pożarnej zgodnie z obowiązującym stanem prawnym jest również zaprojektowany do prowadzenia współpracy międzynarodowej, udziału w przygotowywaniu i wykonywaniu umów międzynarodowych oraz kierowaniu jednostek organizacyjnych Państwowej Straży Pożarnej do akcji ratowniczych i humanitarnych poza granicę państwa, na podstawie wiążących Rzeczpospolitą Polską umów międzynarodowych.

Zbiory tych elementów i funkcji, odpowiednio połączonych ze sobą mają decydujący wpływ na prawidłowe działanie całości. System, jego podsystemy, ich poszczególne elementy ulegają modyfikacjom, są reformowane i przekształcane. Istotą wszelkich zmian —

[3] A. Warmiński, *Zadania i organizacja Państwowej Straży Pożarnej w zakresie ochrony przeciwpożarowej*, DOCTRINA, Akademia Podlaska, Siedlce 2009 s. 276.

[4] K. Wójtowicz, *Organizacja i funkcjonowanie Państwowej Straży Pożarnej w Polsce*, 2012 r., s.16.

przy założeniu, że co do zasady działanie tych systemów jest nacechowane postępowaniem dla dobra państwa, a przede wszystkim na rzecz dobra obywatela, jednostki - jest to postępowanie logiczne, którego skutkiem ma być ulepszenie już istniejącego stanu. Bezpieczeństwo to dobro wspólne, wobec czego systemy, które działają na rzecz bezpieczeństwa, są także dobrem wspólnym.

Aby zrozumieć istotę funkcjonowania systemu wymiany informacji w PSP, ze szczególnym uwzględnieniem krajowego systemu ratowniczo-gaśniczego, w tym też wymiany informacji z centrami, służbami, podmiotami i innymi instytucjami, niezbędnym jest scharakteryzowanie procesów jakie realizowane są przez instytucję publiczną jaką jest Państwowa Straż Pożarna oraz czym jest sama formacja.

Szeroki zakres kompetencji Państwowej Straży Pożarnej zawarty jest w aktach normatywnych, które można podzielić na akty podstawowe regulujące zadania ochrony przeciwpożarowej i Państwowej Straży Pożarnej oraz akty uzupełniające zawierające zasady dotyczące innych dziedzin prawa, ale przyznające jednocześnie określone kompetencje organom Państwowej Straży Pożarnej[5].

Ustawodawca wskazał, że Państwowa Straż Pożarna to zawodowa, umundurowana i wyposażona w specjalistyczny sprzęt formacja, przeznaczona do walki z pożarami, klęskami żywiołowymi i innymi miejscowymi zagrożeniami[6].

Do podstawowych zadań Państwowej Straży Pożarnej należy:

- rozpoznawanie zagrożeń pożarowych i innych miejscowych zagrożeń,
- organizowanie i prowadzenie akcji ratowniczych w czasie pożarów, klęsk żywiołowych lub likwidacji miejscowych zagrożeń,
- wykonywanie pomocniczych specjalistycznych czynności ratowniczych w czasie klęsk żywiołowych lub likwidacji miejscowych zagrożeń przez inne służby ratownicze.

Jednostkami organizacyjnymi Państwowej Straży Pożarnej są[7]:

- Komenda Główna;
- 16 komend wojewódzkich;
- 335 komend powiatowych (miejskich);

[5] K. Fiszer. D. Markiewicz, *Ochrona przed pożarami i innymi nadzwyczajnymi zagrożeniami,* tom I Wyd. ZPP
Warszawa 2008 r. s. 53.

[6] Dziennik Ustaw 2006, nr 96, poz. 667, z późn. zm.

[7] „Biuletyn Informacyjny Państwowej Straży Pożarnej" 2021.

- 5 szkół pożarniczych;
- Centrum Naukowo Badawcze Ochrony Przeciwpożarowej – PIB;
- Centralne Muzeum Pożarnictwa.

Krajowy System Ratowniczo-Gaśniczy stanowi integralną część bezpieczeństwa wewnętrznego państwa, obejmującego cały obszar kraju, w tym wszystkie podmioty ratownicze w celu zachowania bezpieczeństwa pożarowego, technicznego, ekologicznego, chemicznego bez względu na miejsce, rodzaj i charakter ewentualnie prowadzonych działań[8].

Funkcjonowanie krajowego system ratowniczo-gaśniczy umocowane jest prawnie w ustawie z 24 sierpnia 1991 roku o ochronie przeciwpożarowej oraz ustawie z dnia 24 sierpnia 1991 roku o Państwowej Straży Pożarnej.

Definicja systemu jest precyzyjnie określona w przepisie prawa i stanowi, że krajowy system ratowniczo-gaśniczy to integralna część organizacji bezpieczeństwa wewnętrznego państwa, mający na celu ratowanie życia, zdrowia, mienia lub środowiska, prognozowanie, rozpoznawanie i zwalczanie pożarów, klęsk żywiołowych lub innych miejscowych zagrożeń. System skupia jednostki ochrony przeciwpożarowej, inne służby, inspekcje, straże, instytucje oraz podmioty, które dobrowolnie w drodze umowy cywilnoprawnej zgodziły się współdziałać w akcjach ratowniczych. Zaczął funkcjonować od 1995 roku, a jego organizatorem jest Państwowa Straż Pożarna. Podstawowym założeniem w budowie systemu ratowniczo-gaśniczego było stworzenie jednolitego i spójnego układu skupiającego powiązane z sobą różne podmioty ratownicze tak, aby można było skutecznie podjąć każde działanie ratownicze.

Istotnym elementem systemu jest udzielane wsparcie i pomoc dobrowolna ze strony osób fizycznych i prawnych, zwanych podmiotami wspomagającymi. Wspierają one działania jednostek organizacyjnych Państwowej Straży Pożarnej poprzez: udział w ratowaniu ludzi, ich mienia oraz środowiska naturalnego, dostarczanie narzędzi i środków, wykonywanie określonych prac lub zadań wyznaczonych przez organizatora akcji, ograniczenie i eliminowanie skutków zdarzeń i udostępnienie informacji specjalistycznych[9].

System ten to zespół przedsięwzięć organizacyjno-planistycznych, szkoleniowych i materialno-technicznych, realizowanych przez komendantów Państwowej Straży Pożarnej, podległe i podporządkowane im siły i środki, a także inne podmioty, które wchodzą

[8] Z. Radny, *Rozważania wokół Krajowego Systemu Ratowniczo-Gaśniczego,* „Przegląd Pożarniczy" 1995, nr 10, s. 9-10.
[9] J. Żubr vel Michałowski, *Prawne umocowanie systemu*, „Przegląd Pożarniczy" 1995, nr 12, s. 8.

w skład tego systemu. Głównym celem ksrg jest zapewnienie ochrony życia, zdrowia, mienia lub środowiska, w ramach działań podejmowanych przez PSP i inne podmioty ratownicze (ze szczególnym uwzględnieniem OSP), poprzez:

- gaszenie pożarów,
- likwidację innych miejscowych zagrożeń (działania ratownicze),
- ratownictwo chemiczne i ekologiczne,
- ratownictwo techniczne,
- ratownictwo medyczne w zakresie udzielania kwalifikowanej pierwszej pomocy (KPP).

Krajowy system ratowniczo-gaśniczy w ramach posiadanych sił i środków współpracuje z właściwymi organami i podmiotami podczas zdarzeń nadzwyczajnych wywołanych zagrożeniem czynnikiem biologicznym, w tym podczas zdarzeń o charakterze terrorystycznym. Jak wspomniano wcześniej system opiera się na Państwowej Straży Pożarnej, wiodącej i utrzymywanej z budżetu państwa służbie ratowniczej, jak również Ochotniczych Strażach Pożarnych, utrzymywanych z budżetów samorządowych i dotacji z budżetu państwa.

System ratowniczy powinien być zbudowany i stale rozwijany lub przebudowywany w miarę potrzeb. Rozbudowa, czy przebudowa systemu ratowniczego rozumiana jako pokrywanie jego zasięgiem nowych obszarów, udoskonalaniem działań i zwiększaniem sprawności, dostępności systemu i jakości działań ratowniczych musi być właściwie ukierunkowana[10]. Centralnym organem administracji rządowej w sprawach organizacji ksrg oraz ochrony przeciwpożarowej jest Komendant Główny PSP. Podlega on ministrowi właściwemu do spraw wewnętrznych, który pełni nadzór nad funkcjonowaniem ksrg.
W tym zakresie Komendant Główny realizuje związane z kompetencją tego organu zadania o charakterze wykonawczo-zarządzającym, a w szczególności w przedmiocie kierowania Krajowym Systemem Ratowniczo-Gaśniczym (dysponowania podmiotami krajowego systemu i odwodami poprzez swoje stanowisko kierowania, sprawowania inspekcji i nadzoru, analizy działań ratowniczych), analizy zagrożeń pożarowych i innych miejscowych zagrożeń oraz pracy Komendy Głównej, a to oznacza wypełnianie funkcji: planowania, organizowania, stanowienia, stosowania prawa, wytyczania kierunków działania, koordynowania, ustalania zadań nadzoru i kontroli[11].

[10] Praca zbiorowa – *„Ochrona przeciwpożarowa a bezpieczeństwo państwa”*, Wyd. CNBOP-PIB, Józefów 2014 r., s. 17.
[11] Z. Radny, *Komenda Główna Państwowej Straży Pożarnej*, Warszawa 1992, s. 4.

System funkcjonuje na trzech poziomach odpowiadających strukturze administracyjnej kraju:

- powiatowy – podstawowy poziom wykonawczy, gdzie działania prowadzone są przez siły i środki powiatu, gdzie organizacja funkcjonowania ksrg przez komendanta powiatowego (miejskiego) Państwowej Straży Pożarnej, na obszarze powiatu, obejmuje:
  - opracowanie analiz zagrożeń oraz analiz zabezpieczenia operacyjnego;
  - opracowanie powiatowego planu ratowniczego;
  - ustalenie sieci podmiotów ksrg i ich obszarów chronionych;
  - aktualizację danych dotyczących gotowości operacyjnej i podwyższonej gotowości operacyjnej;
  - ustalenie metod powiadamiania w sytuacji wystąpienia nagłego lub nadzwyczajnego zagrożenia;
  - przemieszczanie sił i środków ksrg do czasowych miejsc stacjonowania;
  - ustalenie metod powiadamiania, alarmowania i współdziałania podmiotów podczas działań ratowniczych;
  - wdrożenie systemu dysponowania sił i środków do działań ratowniczych.
- wojewódzki – koordynujący i wspierający działania ratownicze, gdy siły powiatu są niewystarczające, gdzie organizacja funkcjonowania ksrg przez komendanta wojewódzkiego Państwowej Straży Pożarnej, na obszarze województwa, obejmuje:
  - opracowanie analiz zagrożeń oraz analiz zabezpieczenia operacyjnego;
  - opracowanie wojewódzkiego planu ratowniczego;
  - ustalanie obszarów chronionych dla specjalistycznych grup ratowniczych oraz dla podmiotów ksrg przewidzianych do realizacji zadań poza terenem własnego działania;
  - aktualizację danych dotyczących gotowości operacyjnej odwodów operacyjnych na obszarze województwa oraz w ramach pomocy transgranicznej;
  - dysponowanie sił i środków specjalistycznych grup ratowniczych i odwodów operacyjnych na obszarze województwa;
  - ustalanie zasad powiadamiania i współdziałania podmiotów na obszarze województwa podczas działań ratowniczych.
- krajowy – koordynujący i wspierający działania ratownicze, gdy siły województwa są niewystarczające oraz realizujący oficjalne prośby o udzielenie pomocy ratowniczej i humanitarnej poza jego granicami, gdzie organizacja funkcjonowania ksrg przez Komendanta Głównego Państwowej Straży Pożarnej, obejmuje:

- aktualizację danych dotyczących gotowości operacyjnej centralnego odwodu operacyjnego i podmiotów przewidzianych do współdziałania na obszarze kraju i poza jego granicami;
- opracowanie dokumentacji dotyczącej powiadamiania i współdziałania podmiotów na obszarze kraju podczas działań ratowniczych;
- opracowanie dokumentacji dotyczącej organizowania działań ratowniczych;
- opracowanie dokumentacji dotyczącej ewidencjonowania zdarzeń;
- opracowanie dokumentacji dotyczącej organizacji i funkcjonowania systemów teleinformatycznych, w tym na potrzeby kierującego działaniem ratowniczym;
- opracowanie dokumentacji dotyczącej organizacji łączności alarmowania, powiadamiania, dysponowania oraz współdziałania na potrzeby działań ratowniczych;
- opracowanie dokumentacji dotyczącej współpracy podczas działań ratowniczych z nadawcami programów radiowych i telewizyjnych oraz z wolontariuszami, o których mowa w ustawie z dnia 24 kwietnia 2003 r. o działalności pożytku publicznego i o wolontariacie (Dz. U. z 2020 r. poz. 1057 oraz z 2021 r. poz. 1038, 1243 i 1535);
- opracowanie dokumentacji dotyczącej wsparcia psychologicznego osób uczestniczących w działaniach ratowniczych;
- opracowanie dokumentacji dotyczącej tworzenia przez podmioty ksrg wspólnych zespołów ratowniczych;
- opracowanie dokumentacji dotyczącej organizowania ćwiczeń ratowniczych;
- opracowanie dokumentacji dotyczącej podwyższania gotowości operacyjnej;
- opracowanie dokumentacji dotyczącej analizowania zdarzeń;
- opracowanie dokumentacji dotyczącej organizacji krajowych baz sprzętu specjalistycznego i środków gaśniczych;
- opracowanie dokumentacji dotyczącej organizacji działań specjalistycznych grup ratownictwa wodno-nurkowego w ksrg;
- opracowanie dokumentacji dotyczącej organizacji działań poszukiwawczo-ratowniczych w ksrg;
- opracowanie dokumentacji dotyczącej organizacji ratownictwa chemicznego i ekologicznego w ksrg, uwzględniającej współpracę z właściwymi organami i podmiotami podczas zdarzeń nadzwyczajnych wywołanych czynnikiem biologicznym, w tym podczas zdarzeń terrorystycznych, oraz postępowanie w przypadku likwi-

dacji zagrożenia w ramach posiadanych sił i środków, w tym w działaniach ratowniczych, w przypadku wystąpienia zdarzenia radiacyjnego;

- opracowanie dokumentacji dotyczącej organizacji ratownictwa medycznego w ksrg;
- opracowanie dokumentacji dotyczącej organizacji ratownictwa technicznego w ksrg;
- opracowanie dokumentacji dotyczącej organizacji działań specjalistycznych grup ratownictwa wysokościowego w ksrg;
- opracowanie dokumentacji dotyczącej organizacji centralnego odwodu operacyjnego ksrg.

Gotowość operacyjna sił i środków ksrg, w szczególności dyspozycyjność, wyszkolenie i wyposażenie w sprzęt ratowniczy, umożliwia ich dysponowanie w trybie pilnym według kryterium obszaru chronionego, to znaczy sił i środków niezbędnych do likwidacji lub ograniczania powstałego nagłego zagrożenia, mogących przybyć na miejsce zdarzenia w najkrótszym czasie. Zakłada się, że sieć jednostek ochrony przeciwpożarowej umożliwia dotarcie sił ratowniczych do zagrożonej ludności wciągu 15 min. do 85% populacji.
Konstrukcja ksrg zakłada także, że procedury realizacji podstawowych zadań ratowniczych są dostosowane do specyfiki rodzaju zdarzeń, również masowych lub katastrof.
Niezależnie od sieci jednostek ochrony przeciwpożarowej, które są przygotowane w zakresie podstawowym do realizacji zadań w każdej dziedzinie ratownictwa, Państwowa Straż Pożarna posiada w swych zasobach wydzielone siły i środki do realizowania specjalistycznych czynności ratowniczych poprzez wysoce specjalistyczny sprzęt ratowniczy oraz ponadstandardowe wyszkolenie strażaków PSP. Wydzielone zasoby ratownicze skupione są w 174 specjalistycznych grupach ratowniczych. Ponadto wyznaczone siły i środki z obszaru całego kraju skupione są w ramach Centralnego Odwodu Operacyjnego (charakterystyka poniżej). Gdy siły i środki, dysponowane przez stanowisko kierowania Państwowej Straży Pożarnej na poziomie powiatu, podmiotów ksrg i innych podmiotów uczestniczących w działaniu ratowniczym są niewystarczające, czynności ratownicze realizują również siły i środki podmiotów ksrg zadysponowane z obszaru województwa przez właściwego terenowo komendanta wojewódzkiego Państwowej Straży Pożarnej. Natomiast gdy siły i środki podmiotów ksrg dysponowane przez komendanta wojewódzkiego Państwowej Straży Pożarnej są niewystarczające, czynności ratownicze realizują również podmioty ksrg zadysponowane z obszaru kraju przez Komendanta Głównego Państwowej Straży Pożarnej.

Mając na uwadze, że nadrzędnym celem Państwowej Straży Pożarnej jest ratowanie zagrożonego życia ludzkiego i wszelkiego mienia poprzez dotarcie do poszkodowanego w jak najkrótszym czasie, niezbędnym jest posiadanie w całym kraju, optymalnie rozlokowanej sieci: jednostek ratowniczo-gaśniczych oraz wspierających je stanowiska kierowania PSP, połączone między sobą w taki sposób, aby bezpiecznie i jak najszybciej wymieniać stosowne informacje.

W Państwowej Straży Pożarnej funkcjonują 504 Jednostki Ratowniczo-Gaśnicze PSP - 499 w strukturach komend powiatowych (miejskich) PSP oraz 5 w szkołach PSP – co daje ok. 5100 strażaków (codziennie na 24 godzinnej służbie) i ok. 5300 samochodów ratowniczo-gaśniczych i specjalnych.

W krajowym systemie ratowniczo-gaśniczym mamy 4777 jednostek Ochotniczych Straży Pożarnych - ok. 11 300 samochodów ratowniczo-gaśniczych i specjalnych.

Wyznaczone siły i środki z obszaru całego kraju skupione są w ramach centralnego odwodu operacyjnego ksrg w:

- kompaniach gaśniczych,
- kompaniach specjalnych,
- pododdziałach logistycznych,
- specjalistycznych grupach ratowniczych,
- kompaniach szkolnych.

Poniżej przedstawiono aktualne zestawienie pododdziałów włączonych do centralnego odwodu operacyjnego ksrg.

Tabela 3-1
Skład centralnego odwodu operacyjnego ksrg.

Rodzaj pododdziałów	**Liczba**
Kompanie gaśnicze, w skład których wchodzą:	22
Pluton typu „A” (pluton samochodów gaśniczych)	44
Pluton typu „B” (pluton ciężkich samochodów gaśniczych)	19
Pluton typu „C” (wsparcia)	22
Pluton typu „D” (pluton ciężkich samochodów gaśniczych z DWP)	20

Źródło: Biuletyn Informacyjny PSP 2021 r.

Tabela 3-1 cd.
Skład centralnego odwodu operacyjnego ksrg.

Rodzaj pododdziałów	Liczba
Kompanie specjalne, w skład których wchodzą:	31
Sekcja typu „A” (sekcja ewakuacyjna)	36
Sekcja typu „B” (sekcja pomp dużej wydajności)	32
Sekcja typu „C” (sekcja pomp szlamowych)	22
Sekcja typu „D” (sekcja przeciwpowodziowa z zaporami)	12
Sekcja typu „E” (sekcja zapasowego zasilania energetycznego)	16
Sekcja typu „F” (sekcja przeciwpowodziowa z łodziami	11
Sekcja typu „G” (sekcja z pompą o wydajności powyżej 40000 dm^3/min	10
Pluton typu „H” (sekcja przeciwpowodziowa z łodziami	32
Pododdziały logistyczne, w skład których wchodzą:	16
Kompania logistyczna	1
Pluton logistyczny	15
Grupy specjalistyczne, w skład których wchodzą:	183
Specjalistyczne grupy ratownictwa wodno-nurkowego	48
Specjalistyczne grupy ratownictwa wysokościowego	32
Specjalistyczne grupy ratownictwa chemiczno-ekologicznego	49
Specjalistyczne grupy ratownictwa technicznego	24
Specjalistyczne grupy poszukiwawczo-ratownicze	21
Specjalistyczne grupy sonarowe	9
Moduły ratownicze do działań międzynarodowych, w skład których wchodzą:	20
Moduł gaszenia pożarów lasów z ziemi z użyciem pojazdów	6
Moduł pomp wysokiej wydajności	4
Moduł wykrywania skażeń chemicznych, biologicznych, radiologicznych i jądrowych oraz pobierania próbek	4
Moduł grupy poszukiwawczo-ratowniczej przeznaczonej do działań na terenach miejskich	6
Kompanie szkolne	5

Źródło: Biuletyn Informacyjny PSP 2021 r.

W strukturach PSP funkcjonuje pięć szkół pożarniczych, w których Komendant Główny PSP utworzył kompanie szkolne w ramach centralnego odwodu operacyjnego krajowego systemu ratowniczo-gaśniczego. Dostępność słuchaczy szkół jest codziennie monitorowana przez Stanowisko Kierowania Komendanta Głównego PSP, gdyż mogą być oni zadysponowani do działań na terenie kraju – ogółem 1037 strażaków:

- Szkoła Główna Służby Pożarniczej w Warszawie – 371 strażaków;
- Centralna Szkoła Państwowej Straży Pożarnej w Częstochowie – 152 strażaków;
- Szkoła Aspirantów Państwowej Straży Pożarnej w Poznaniu – 147 strażaków;
- Szkoła Aspirantów Państwowej Straży Pożarnej w Krakowie – 176 strażaków;
- Szkoła Podoficerska Państwowej Straży Pożarnej w Bydgoszczy – 191 strażaków.

Państwowa Straż Pożarna posiada w swych zasobach wydzielone siły i środki do realizowania specjalistycznych czynności ratowniczych poprzez odpowiednio wyszkolonych strażaków Państwowej Straży Pożarnej z wykorzystaniem specjalistycznego sprzętu ratowniczego. Ich rozkład w poszczególnych województwach przedstawiono poniżej w tabeli:

Tabela 3-2
Wydzielone SIS do czynności specjalistycznych.

Lp.	Województwo/ Szkoła PSP	Specjalistyczne Grupy Poszukiwawczo – Ratownicze (SGPR)	Specjalistyczne Grupy Ratownictwa Chemiczno – Ekologicznego (SGRChem)	Specjalistyczne Grupy Ratownictwa Technicznego (SGRT)	Specjalistyczne Grupy Ratownictwa Wysokościowego (SGRW)	Specjalistyczne Grupy Ratownictwa Wodno – Nurkowego (SGRWN)
1.	Dolnośląskie	3	3	2	3	4
2.	Kujawsko - Pomorskie	1	3	2	1	2
3.	Lubelskie	1	3	1	1	1
4.	Lubuskie	1	2	1	2	2
5.	Łódzkie	1	2	1	1	3
6.	Małopolskie	2	5	3	3	3
7.	Mazowieckie	1	6	1	5	5
8.	Opolskie	1	2	1	2	1
9.	Podkarpackie	1	2	1	2	3
10.	Podlaskie	1	1	1	1	4
11.	Pomorskie	1	3	2	2	4
12.	Śląskie	2	4	2	2	1
13.	Świętokrzyskie	1	3	1	1	1
14.	Warmińsko - Mazurskie	1	3	1	2	8
15.	Wielkopolskie	1	5	1	2	4
16.	Zachodniopomorskie	2	2	2	2	2
17.	Centrala Szkoła PSP w Częstochowie	0	0	1	0	0
RAZEM		**21**	**49**	**24**	**32**	**48**

Źródło: Biuletyn Informacyjny PSP 2021 r.

Ponadto, do ksrg włączane są również jednostki ochrony przeciwpożarowej innych służb i podmiotów:

- 5 Zakładowych Straży Pożarnych;

- 1 Zakładowa Służba Ratownicza;
- 2 Lotniskowe Służby Ratowniczo-Gaśnicze;
- 21 jednostek Wojskowej Ochrony Przeciwpożarowej.

W ramach krajowego systemu ratowniczo-gaśniczego z Państwową Strażą Pożarną współpracuje szereg służb, podmiotów i instytucji, które wspierają jednostki ochrony przeciwpożarowej w działaniach. System wpierany jest przez m.in.:

- Policję;
- Państwowe Ratownictwo Medyczne;
- Lotnicze Pogotowie Ratunkowe;
- Straż Graniczną;
- Siły Zbrojne RP;
- Służbę Celno–Skarbową;
- Morską Służbę Poszukiwania i Ratownictwa;
- Inspekcję Ochrony Środowiska;
- Górskie Ochotnicze Pogotowie Ratunkowe;
- Państwową Inspekcję Sanitarną;
- Państwową Inspekcję Weterynaryjną;
- Polski Czerwony Krzyż;
- Związek Harcerstwa Polskiego;
- Aeroklub Polski;
- Wodne Ochotnicze Pogotowie Ratunkowe;
- Centralną Stację Ratownictwa Górniczego;
- Państwowa Agencja Atomistyki;
- Instytut Meteorologii i Gospodarki Wodnej;
- Inspekcję Ochrony Środowiska;
- Państwową Inspekcję Pracy;
- Nadzór Budowlany;
- Urząd Dozoru Technicznego.

W ustawie o Państwowej Straży Pożarnej, jako jedno z zadań podstawowych PSP, wskazano współdziałanie ze strażami pożarnymi i służbami ratowniczymi innych państw oraz ich organizacjami międzynarodowymi na podstawie wiążących Rzeczpospolitą Polską umów międzynarodowych oraz odrębnych przepisów, a także realizację innych zadań

wynikających z wiążących Rzeczpospolitą Polską umów międzynarodowych na zasadach i w zakresie w nich określonych. Ponadto, do zadań Komendanta Głównego PSP należy prowadzenie współpracy międzynarodowej, udział w przygotowywaniu i wykonywaniu umów międzynarodowych w zakresie określonym w ustawach i w tych umowach oraz kierowanie jednostek organizacyjnych Państwowej Straży Pożarnej do akcji ratowniczych i humanitarnych poza granicę państwa, na podstawie wiążących Rzeczpospolitą Polską umów międzynarodowych.

W zasadach organizacji centralnego odwodu operacyjnego krajowego systemu ratowniczo-gaśniczego, zwanych dalej Zasadami, ujęto polskie moduły ochrony ludności, jako moduły ratownicze do działań międzynarodowych. Zaznaczono, iż w przypadku tworzenia modułów ratowniczych do działań międzynarodowych dopuszcza się by ich skład pokrywał się ze składem pozostałych pododdziałów włączonych w struktury.

Moduły ratownicze do działań międzynarodowych, przeznaczone są do prowadzenia działań ratowniczych poza granicami Rzeczypospolitej Polskiej.

Koszty tworzenia i utrzymania Modułów ponoszą właściwi komendanci wojewódzcy/ miejscy/ powiatowi i szkół Państwowej Straży Pożarnej. Koszty udziału Modułów w działaniach ratowniczych i ćwiczeniach poza granicami Rzeczypospolitej Polskiej w zakresie: diet, ubezpieczenia dla ratowników, wyżywienia oraz paliwa ponosi Komendant Główny Państwowej Straży Pożarnej. Koszty odtworzenia sprzętu Modułów biorących udział w działaniach ratowniczych i ćwiczeniach poza granicami Rzeczypospolitej Polskiej ponosi komenda wojewódzka PSP lub szkoła PSP.

W przypadku braku możliwości zapewnienia środków finansowych przez daną komendę wojewódzką PSP lub szkołę PSP na pokrycie kosztów, po wykorzystaniu wszystkich dostępnych źródeł finansowania, Komendant Główny PSP podejmuje decyzje odnośnie odtworzenia sprzętu w Module.

Moduły tworzone są w taki sposób by wypełnić wymagania określone we właściwej Decyzji Komisji Europejskiej ustanawiającej Mechanizm Wspólnotowy Unii Europejskiej ułatwiający wzmocnioną współpracę w interwencjach wspierających ochronę ludności. Dane o utworzonych Modułach rejestrowane są w elektronicznym systemie CECIS na stanowisku kierowania Komendanta Głównego Państwowej Straży Pożarnej. Dysponowanie Modułów do prowadzenia działań poza granicami kraju odbywa się na podstawie „Planu najbardziej prawdopodobnego dysponowania modułów", który zatwierdzany jest przez Komendanta Głównego PSP lub dowódcę COO.

Państwowa Straż Pożarna posiada następujące moduły ochrony ludności:

- HUSAR lub MUSAR (moduł grupy poszukiwawczo-ratowniczej przeznaczonej do działań na terenach miejskich w konfiguracji ciężkiej lub średniej) - 7 SGPR (Warszawa, Gdańsk, Poznań, Nowy Sącz, Łódź, Wałbrzych, Jastrzębie Zdrój);
- HCP (moduł pomp wysokiej wydajności) – 4 moduły (Katowice, Toruń, Rzeszów, Gorzów Wlkp.),
- GFFFV (moduł gaszenia pożarów lasów z ziemi z użyciem pojazdów) – 6 modułów (Kraków, Białystok, Poznań, Olsztyn, Szczecin, Wrocław),
- CBRN (moduł wykrywania skażeń chemicznych, biologicznych, radiologicznych i nuklearnych oraz pobierania próbek) – 4 moduły (Warszawa, Katowice, Kraków, Poznań).

3.2 CHARAKTERYSTYKA SYSTEMÓW I ELEMENTÓW WYMIANY INFORMACJI FUNKCJONUJĄCYCH W PAŃSTWOWEJ STRAŻY POŻARNEJ.

Znaczącą rolę w procesie ratownictwa i ochrony ludności, ze szczególnym uwzględnieniem, w jedną stronę kontaktu z obywatelem, a w drugą ze strażakami udzielającymi pomocy pełnia stanowiska kierowania Państwowej Straży Pożarnej. To w tych miejscach strażak prowadzi rozmowy z roztrzęsionymi dzwoniącymi ludźmi, wyłuskuje z nich najistotniejsze informacje, choć często są one szczątkowe, a następnie podejmuje błyskawiczne decyzje, często w stresie, by precyzyjnie przyjąć zgłoszenie, a następnie zadysponować do zdarzenia właściwe siły i środki. Tak można opisać zbiór elementów składających się na specyfikę służby w stanowisku kierowania.

Kierujący na stanowisku odpowiada za dysponowanie sił i środków do działań z uwzględnieniem rodzaju, wielkości zdarzenia i liczby poszkodowanych, dlatego dużą rolę dla niego ma bieżący kontakt z miejscem zdarzenia w celu posiadania informacji do prawidłowego oddziaływania na ratowników i niepopełnienia błędów[12].

Dyspozytor to osoba, która jest odpowiedzialna za efektywne i optymalne zarządzanie ludźmi, sprzętem i informacjami. Zawód dyspozytora dzieli się na różne obszary w zależności od profilu działalności. Najbardziej rozpowszechniona jest działalność dys-

[12] A. Warmiński, Zadania *i organizacja*…, op.cit., s. 279

pozytora medycznego i transportu, jednak lista jest zdecydowanie obszerniejsza, dyspozytor służb ratunkowych (alarmowy), dyspozytor policji, czy też właśnie dyspozytor pożarnictwa[13].

Służba w SK często identyfikowana jest jako praca na specyficznym odcinku, wymagającym znacznej odporności na stres, podejmowania szybkich decyzji oraz zdolności przewidywania dalszego rozwoju sytuacji na miejscu zdarzenia. Organizacyjnie w większości SK służba pełniona jest w systemie 24/48 godz. Zdecydowana większość powiatowych oraz niektóre miejskie stanowiska kierowania posiadają obsadę jednoosobową, co oznacza, że funkcyjny przez 24 godz. musi być zdolny do wykonywania czynności związanych z przyjmowaniem zgłoszeń alarmowych, ich weryfikacją, dysponowaniem SIS jednostek ochrony przeciwpożarowej do zdarzeń oraz koordynacją działań ratowniczych, w które zaangażowane są SIS. Co istotne, dyżurni SK stanowią nieocenione wsparcie dla strażaków podczas prowadzenia działań ratowniczo-gaśniczych na miejscu zdarzenia:

- zapewniają bieżącą weryfikację informacji na potrzeby Kierującego Działaniem Ratowniczym (KDR);
- dysponują dodatkowe SIS z podległych jednostek;
- zgodnie z zapotrzebowanie KDR, występują do nadrzędnych SK PSP o dodatkowe SIS z innych powiatów lub województw;
- angażują w akcje inne podmioty (za pośrednictwem stanowisk kierowania innych służb lub właściwych terenowo centrów zarządzania kryzysowego), których potencjał jest niezbędny do właściwego prowadzenia działań (np. wyspecjalizowany sprzęt techniczny);
- organizują zabezpieczenie logistyczne działań, w tym na potrzeby ewakuowanej ludności,

Zgodnie z obowiązującym stanem prawnym do zadań stanowisk kierowania na wszystkich poziomach należy:

- przyjmowanie, kwalifikowanie oraz w razie potrzeby, przekazywanie zgłoszeń alarmowych;
- dysponowanie zasobów ratowniczych do działań ratowniczych;
- wspomaganie i koordynacja działań ratowniczych;
- bieżące analizowanie:
  - informacji o zagrożeniach z systemów monitoringu podmiotów ksrg,

[13] Encyklopedia Zarządzania - *https://mfiles.pl/pl/index.php/Strona_g%C5%82%C3%B3wna.*

- gotowości operacyjnej,
- czasu interwencji, w tym czasu dysponowania, przybycia, prowadzenia i zakończenia działań ratowniczych – czas interwencji, rozumiano jako łączny czas trwania działań, liczony od chwili przyjęcia zgłoszenia o zdarzeniu przez stanowisko kierowania komendanta Państwowej Straży Pożarnej do czasu powrotu ostatnich sił i środków podmiotów ksrg do miejsca stacjonowania,
- przebiegu działań ratowniczych,
- rezerw materiałowych i sprzętowych podmiotu ksrg;

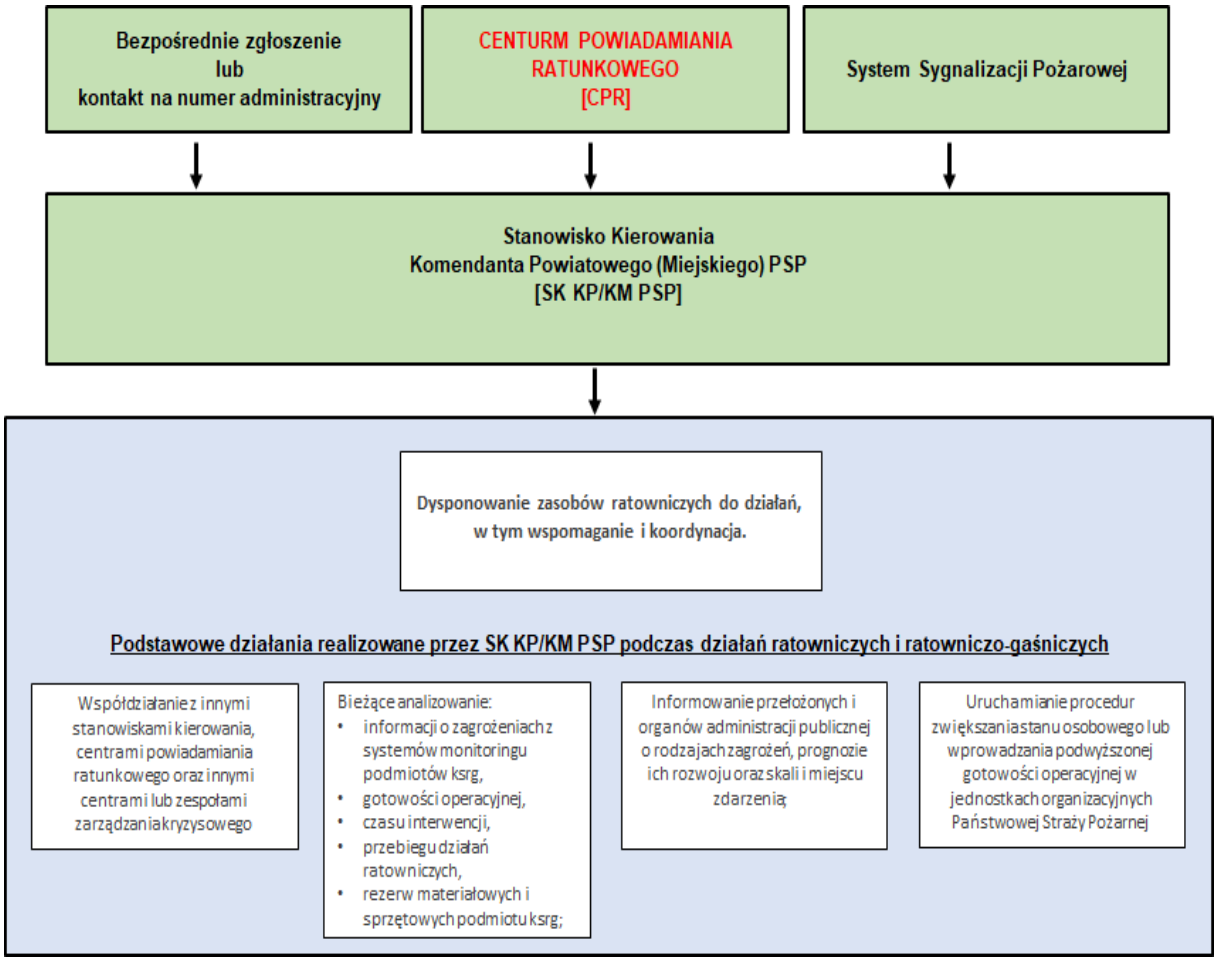
- informowanie przełożonych i organów administracji publicznej o rodzajach zagrożeń, prognozie ich rozwoju oraz skali i miejscu zdarzenia;
- uruchamianie procedur zwiększania stanu osobowego lub wprowadzania podwyższonej gotowości operacyjnej w jednostkach organizacyjnych Państwowej Straży Pożarnej;
- uruchamianie awaryjnych planów ewakuacji osób pełniących służbę w stanowisku kierowania oraz sprzętu technicznego w miejsca zastępcze;
- współdziałanie ze stanowiskami kierowania, centrami powiadamiania ratunkowego oraz innymi centrami lub zespołami zarządzania kryzysowego;
- współdziałanie z grupami ratowniczymi wykonującymi zadania poza granicami państwa;
- korzystanie z map, systemów informatycznych oraz innych narzędzi niezbędnych do analizowania i prognozowania zagrożeń, a także do tworzenia i aktualizowania baz danych taktycznych i operacyjnych stosowanych podczas organizowania i prowadzenia działań ratowniczych oraz wspomagania procesów decyzyjnych;
- korzystanie z planów ratowniczych oraz innej dokumentacji wykorzystywanej podczas organizowania, prowadzenia i analizowania działań ratowniczych, organizacji odwodów operacyjnych lub wdrażania procedur właściwych dla zarządzania kryzysowego;
- przechowywanie dokumentacji i danych dotyczących przebiegu działań ratowniczych.

W stanowiskach kierowania PSP wszystkich szczebli zapewnia się:

- urządzenia do rejestrowania treści zgłoszeń alarmowych,
- czasu oczekiwania na nawiązanie połączenia,
- czasu przyjęcia zgłoszenia, czasu obsługi zgłoszenia oraz korespondencji prowadzonej w stanowisku kierowania;

- automatyczne systemy zapewniające alarmowanie lub dysponowanie sił i środków oraz bieżące nadzorowanie gotowości operacyjnej;
- sprzęt i aparaturę do pozyskiwania oraz przetwarzania informacji na potrzeby działań ratowniczych;
- zasilanie awaryjne i gwarantowane.

Poniżej przedstawiono schemat obiegu informacji:



Źródło: Opracowanie własne.

Rysunek 3-1
Schemat obiegu informacji w stanowisku kierowania PSP

Na podstawie rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 18 lutego 2011 r. w sprawie szczegółowych zasad organizacji krajowego systemu ratowniczo-gaśniczego opracowane zostały „*Zasady ewidencjonowania zdarzeń w systemie SWD – PSP.*" Powyższy dokument składa się z czterech części. Pierwsza i druga określają szczegółowe zasady prowadzenia wybranej dokumentacji zdarzeń, czasookres jej sporządzania, przesyłania, tryb kontroli poprawności, wprowadzania zmian w informacji ze zda-

rzenia przez stanowiska kierowania komendanta powiatowego/miejskiego, komendanta wojewódzkiego Państwowej Straży Pożarnej oraz osoby odpowiedzialne za sporządzanie poszczególnych elementów dokumentacji. Trzecia część opracowania określa zasady sporządzania informacji ze zdarzenia, zaś czwarta wybrane problemy związane ze sporządzaniem informacji.

Stanowisko kierowania komendanta powiatowego (miejskiego) PSP sporządza[14]:

- kartę zdarzenia,
- zestawienie dobowe zdarzeń.
- przekazuje wstępną informację o zdarzeniu do SK KW PSP, które informuje SK KG PSP w przypadku zdarzeń:

– podczas których wypadkowi uległ ratownik podmiotu ratowniczego;
– podczas których zaistniał wypadek śmiertelny lub doszło do obrażeń ciała u więcej niż 3 osób (do tej liczby należy zaliczyć wszystkich poszkodowanych, w tym przekazanych jednostkom ochrony zdrowia przed przybyciem jednostek ochrony przeciwpożarowej - JOP);
– w których konieczna była ewakuacja co najmniej 10 osób (do tej liczby należy zaliczyć wszystkich ewakuowanych, a nie tylko w rozumieniu kwalifikowanej pierwszej pomocy (KPP), w tym przed przybyciem JOP);
– w których w bezpośrednim działaniu ratowniczym uczestniczyło co najmniej 12 zastępów JOP;
– w których uczestniczyły co najmniej 3 zespoły ratownictwa medycznego (w trakcie obecności na miejscu zdarzenia JOP);
– podczas których dysponowano śmigłowiec lub samolot do prowadzenia działań ratowniczych;
– z udziałem chemicznych, biologicznych, radiologicznych, wybuchowych lub nuklearnych substancji niebezpiecznych stanowiących bezpośrednie zagrożenie dla życia;
– podczas których dysponowano siły i środki odwodu operacyjnego na obszarze województwa lub centralnego odwodu operacyjnego lub korzystano z wiedzy ekspertów do spraw prognozowania zagrożeń lub specjalistów do spraw ratownictwa;

[14] Ramowe Wytyczne Komendant Głównego PSP „*Do Opracowania Zasad Dysponowania Sił Jednostek Ochrony Przeciwpożarowej”*, Warszawa 2013 r.

- podczas których dysponowano siły i środki z państw sąsiednich lub zachodziła konieczność uruchamiania procedur informowania i ostrzegania podczas wystąpienia zagrożeń transgranicznych;
- podczas których wystąpiła poważna awaria w rozumieniu przepisów prawa ochrony środowiska;
- w placówkach dyplomatycznych (w tym poza placówkami, a z udziałem korpusu dyplomatycznego);
- w których wystąpiło zagrożenie niezidentyfikowane w procesie analizy zagrożeń albo inne nadzwyczajne zagrożenie, w tym atak terrorystyczny.

Informację o zadysponowaniu sił i środków do zdarzenia SK KP(M) PSP niezwłocznie przekazuje do SK KW PSP. Informacja o zadysponowanych siłach i środkach przekazywana jest automatycznie przez system SWD PSP. Jednocześnie, dyżurny SK przekazuje tą informację drogą telefoniczną do stanowiska kierowania PSP poziomu wyższego.

Stanowisko kierowania PSP odnotowuje w karcie zdarzenia (karta manipulacyjna w systemie SWD PSP) zakres zadań własnych zrealizowanych w ramach koordynacji działań ratowniczych, zakresu wynikającego z planu ratowniczego oraz zadań wynikających z decyzji, poleceń i rozkazów.

Kierujący Działaniem Ratowniczym (KDR) sporządza informację ze zdarzenia (IzZ), niezwłocznie po zakończeniu działań. W uzasadnionych przypadkach, np. gdy KDR jest dowódca z OSP, informację taką sporządza dyżurny stanowiska kierowania lub dyżurny Punktu Alarmowego Jednostki Ratowniczo-Gaśniczej (PA JRG) w porozumieniu z KDR.

W terminie do 7 dni od zakończenia interwencji KDR może dokonywać zmian lub uzupełnień w IzZ. Po upływie 7 dni dostęp do edycji IzZ zostaje zablokowany przez system. W szczególnych przypadkach istnieje możliwość odblokowania dostępu do IzZ, celem dokonania zmian, po uzyskaniu akceptacji właściwego Komendanta Wojewódzkiego PSP (za pośrednictwem stanowiska kierowania KW PSP).

SK KP(M) PSP po sprawdzeniu poprawności IzZ zatwierdza ją w systemie SWD PSP.

SK KW PSP po sprawdzeniu poprawności IzZ, przesłanej przez SK KP(M) PSP, zatwierdza ją w systemie SWD PSP.

Zestawienie dobowe zdarzeń za dany dzień sporządza się w systemie SWD PSP na potrzeby własne stanowiska kierowania Komendanta PSP, do godz. 0:30 dnia następnego.

W oparciu o IzZ Komendy Powiatowe/Miejskie, Komendy Wojewódzkie, Komenda Główna PSP sporządzają zestawienia statystyczne oraz inne, ograniczone zakresem bazy danych systemu SWD PSP.

Dokumentację zdarzeń określoną rozporządzeniem przechowują właściwe terenowo Komendy Powiatowe/Miejskie PSP.

W systemie SWD PSP generuje się w sposób automatyczny statystyki okresowe, obejmujące zakres informacyjny przedstawiony w module EWID, Zestawienia dobowe. W systemie SWD PSP generuje się w sposób automatyczny statystyki roczne, uwzględniające tabele stałe i dodatkowe modułu Zestawienia-ST.

Jeśli działania realizowane są na:

- terenie kraju, (SK KP/KM PSP) postępuje zgodnie z „Zasadami dysponowania sił jednostek ochrony przeciwpożarowej oraz zasad doraźnego zabezpieczenia operacyjnego terenu powiatu po zadysponowaniu zasobów ratowniczych”,
- poza granicami kraju w ramach udzielanej pomocy przygranicznej lub regionalnej, (SK KP/KM PSP) postępuje zgodnie z zapisami właściwych Instrukcji metodycznych, stanowiące doprecyzowanie postanowień Umów międzypaństwowych odnoszących się do współpracy i wzajemnej pomocy w przypadku katastrof, klęsk żywiołowych i innych poważnych wypadków

W związku z powyższym informacje dotyczące wystąpienia lub podejrzenia wystąpienia nagłego zagrożenia życia lub zdrowia, a także nagłego zagrożenia środowiska lub mienia, kierowane są do SK KP/KM PSP w następujący sposób:

- dla działań na terenie kraju, poprzez:
  - Centra Powiadamiania Ratunkowego (obsługa numerów alarmowych 112 i 998),
  - bezpośrednie lub telefoniczne zgłoszenia alarmowe np. na numer administracyjny stanowiska kierowania,
  - zewnętrzne systemy monitoringu pożarowego.
- dla działań poza granicami kraju, poprzez:
  - stanowiska kierowania komendantów wojewódzkich PSP, dla województw przygranicznych, stanowiące właściwe punkty kontaktowe dla swoich zagranicznych odpowiedników w zakresie organizacji pomocy międzynarodowej na poziomie regionalnym oraz dla wszystkich województw w kontekście dysponowania SIS PSP, zgodnie z dyspozycjami SK KG PSP na potrzeby organizacji wyjazdów grup ratowniczych PSP w ramach udzielania pomocy międzynarodowej.

Celem realizacji wyżej wymienionych zadań, w szczególności pod kątem skrócenia do maksimum czasu reakcji PSP na zgłoszenie alarmowe, niezbędnym jest posiadanie odpowiednich systemów teleinformatycznych, telefonicznych i radiowych, wspomagających działanie organizacji, które odpowiednio są umocowane prawnie, a także zabezpieczone przed dostępem osób trzecich. Przekazywanie informację należy traktować jako część organizacyjną akcji ratowniczej.

W powyższym świetle niezwykle istotne są następujące kwestie:

- przekazywanie danych na odległość,
- twórca informacji,
- odbiorca informacji
- rozumienie danych.

Każda akcja ratunkowa rozpoczyna się bowiem zaalarmowaniem służb przez obywateli, czyli przekazaniem zinterpretowanych danych (informacji), zrozumiałych dla obu stron, za pomocą środków teletechnicznych przez twórcę informacji do jej odbiorcy.

Mając na uwadze znaczenie informacji dla całego procesu ratowniczego, należy wskazać też właściwości informacji, takie jak:

- celowość,
- rzetelność,
- aktualność,
- kompletność,
- wszechstronność,
- odpowiednia dokładność,
- uzasadnione nakłady.

Oprócz nich informacja ma również cechy jakościowe, które wskazał model audytu systemów informacyjnych COBIT, czyli podatność informatyczna mówiąca o słabość danego systemu informatycznego wynikającej z błędów wewnętrznych lub błędów użytkownik[15], do których można zaliczyć:

- efektywność (relacja uzyskanych efektów do poniesionych nakładów),
- wydajność (zdolność do przesyłania i przetwarzania określonej ilości informacji w jednostce czasu),
- poufność (wykorzystywanie tylko przez uprawnione osoby),
- integralność (nienormalizowane i niemodyfikowane),

[15] Encyklopedia zarządzania - wersja online, hasło *System informacyjny*, (dostęp 2023-02-16).

- dostępność (zgodnie z zasadami wiedzy uzasadnionej),
- wiarygodność (oznaczenie stopnia zbliżenia do prawdy),
- autentyczności (możliwość zidentyfikowania podmiotu dostarczającego dane)
- rozliczalności (możliwość identyfikowania użytkownika oraz zakresu dostępnych dla niego informacji),
- niezaprzeczalności (użytkownik zweryfikowany w dostępie do procesu informatycznego)
- niezawodności (bezawaryjne działanie zapewniające stały dostęp w ustalonych przedziałach czasu).

W zakresie identyfikacji zasobów informacji w kontekście funkcji możemy wyróżnić następujące cechy:

- informacyjną, odpowiedzialnej za rozpoznanie możliwości i potrzeb odbiorcy
- decyzyjną, dokonanie wyboru przez wariantowanie
- motywująco-sterującą, wywołującej określonej reakcji u odbiorcy, wpływającej na zmianę otoczenia
- modelującą, obrazującej przepływ informacji w ramach organizacji.

Konieczność przetwarzania informacji, którą charakteryzują zaprezentowane cechy, zrodziła potrzebę budowy systemów teleinformatycznych, za pomocą których komunikaty te mogą być przekazywane na duże odległości w możliwie najkrótszym czasie.
Zasoby informacyjne postrzegane jako strategiczny zasób organizacji oraz czynnik określający skuteczność procesów oraz środek sterowania, kierowania czy zarządzania wymagają odpowiedniego poziomu bezpieczeństwa.

Podstawowymi narzędziami przekazywania informacji w krajowym systemie ratowniczo-gaśniczym są systemy teleinformatyczne, w szczególności System Wspomagania Decyzji Państwowej Straży Pożarnej (SWD PSP), a także łączność radiowa i telefoniczna.

Znaczenie łączności dla poprawnej koordynacji działań różnego rodzaju służb już w 1929 roku zauważył marszałek Józef Piłsudski, który o łączności wypowiedział się następująco:
„Łączność w wojsku podczas wojennych wypadków jest taką samą bronią jak armata, karabin maszynowy, jak kuchnia polowa, jak wóz amunicyjny kompanji. […] Bez łączności bowiem nie ma i być nie może skoordynowanej pracy wojska, nie ma złączenia wysiłków krwawych żołnierza dla odniesienia zwycięstwa i krew ludzka leje się darmo, leje się nie-

potrzebnie […]. Dlatego też powtarzać zawsze będę, że lepsza jest dobra łączność, niż armata, niż karabin maszynowy, niż kuchnia polowa i wóz amunicyjny[16].

Marszałek Piłsudski zauważył zarówno, jak ważne dla osiągnięcia celów taktycznych i strategicznych są rzetelne i aktualne komunikaty prawidłowo przekazywane w odpowiednim czasie.

Informacje muszą być sprawnie wymieniane na każdym etapie prowadzenia działań ratowniczych czy ich koordynacji. Każda ze służb i instytucji wchodzących w skład krajowego systemu ratowniczo-gaśniczego, a bardziej globalnie w skład Systemu Powiadamiania Ratunkowego, do prawidłowego wykonywania swoich zadań potrzebuje innego rodzaju danych. Dlatego też każda z instytucji dysponuje innym systemem zawierającym nieco odmienne informacje przydatne z jej punktu widzenia. Chcąc pogodzić ze sobą mnogość tych systemów, a w konsekwencji móc je ze sobą połączyć budowane są wspólne interfejsy komunikacyjne.

Interfejsy te obejmują:

- środki do wyświetlania informacji, wyświetlane informacje, formaty i kody;
- tryby poleceń, język - "interfejs użytkownika";
- urządzenia i technologie do wprowadzania danych;
- dialogi, interakcje i transakcje między użytkownikiem a komputerem, informacje zwrotne od użytkownika;
- wsparcie procesu decyzyjnego w konkretnym obszarze tematycznym;
- procedura korzystania z programu i dokumentacja dla niego.

Interfejs użytkownika jest często rozumiany tylko jako wygląd programu czy aplikacji. Jednak w praktyce użytkownik postrzega przez niego cały program jako całość, co oznacza, że to zrozumienie jest zbyt wąskie. W rzeczywistości interfejs użytkownika łączy wszystkie elementy i komponenty programu, które mogą wpływać na interakcję użytkownika z oprogramowaniem, a nie tylko na ekranie, który widzi użytkownik.

Elementy te obejmują:

- zestaw zadań użytkownika, które rozwiązuje przy pomocy systemu;
- metafory używane przez system (na przykład pulpit w MS Windows®);
- elementy sterowania systemem;
- nawigacja między blokami systemu;
- wizualny (i nie tylko) projekt ekranów programu;

[16] Józef Piłsudski rozkaz z 27 marca 1929 o łączności (sygn. archiw.: CAW, akta GISZ, tecz. 518/2). Źródło: „Polityka” nr 11 (2236), 11 marca 2000, s. 86.

- środki do wyświetlania informacji, wyświetlanych informacji i formatów;
- urządzenia i technologie do wprowadzania danych;
- dialogi, interakcje i transakcje między użytkownikiem a komputerem;
- informacja zwrotna od użytkownika;
- wsparcie procesu decyzyjnego w konkretnym obszarze tematycznym;
- jak korzystać z programu i dokumentacji do niego.

Na podstawie powyższego można zauważyć, że w alarmowaniu mamy do czynienia z różnymi systemami teleinformatycznymi. Ich różnorodność wynika ze skomplikowanej struktury samych zagrożeń, a także zaangażowanych sił i środków służących do ich neutralizacji.

W działaniach ratowniczych są używane systemy teleinformatyczne, które ze względu na twórców i odbiorców informacji można podzielić na systemy[7]:

- alarmowania służb ratunkowych przez obywateli, służące do informowania służb o sytuacji zagrożenia zdrowia i życia obywateli;
- korespondencji w akcjach ratunkowych, które służą do komunikacji i wymiany danych pomiędzy służbami ratunkowymi będącymi na miejscu zdarzenia;
- alarmowania ludności przez służby ratunkowe, które służą do przekazywania obywatelom informacji o zagrożeniach i niebezpieczeństwach.

Pojęcie systemu teleinformatycznego w prawodawstwie polskim zostało scharakteryzowane w Ustawie z dnia 22 listopada 2013 r. o systemie powiadamiania ratunkowego. Zgodnie z definicją system teleinformatyczny to zespół współpracujących z sobą urządzeń informatycznych i oprogramowania, zapewniający przetwarzanie i przechowywanie, a także wysyłanie i odbieranie danych poprzez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci urządzenia końcowego[17].

W związku z powyższym zasadnym byłoby dokonać rozdziału ogółu systemów teleinformatycznych na systemy telekomunikacyjne, zapewniające możliwość przekazywania komunikacji i systemy informatyczne służące do przekazywania danych.
System ten zatem realizuje następujące cele: przetwarzanie danych (jak systemy informatyczne) oraz przekazywanie danych na odległość pomiędzy systemami, które przetwarzają dane (jak systemy telekomunikacyjne)[18].
System teleinformatyczny obejmuje:

[17] Ustawi z dnia 22 listopada 2013 r. *O systemie powiadamiania ratunkowego* (Dz. U. 2013 poz. 1635 z późn. zm.).
[18] A. Sobczyk, *Telepraca w prawie polskim*, Wydawnictwo Wolters Kluwer, Warszawa 2009 r., s. 32.

- elementy skoncentrowane – czyli system informatyczny jako zespół urządzeń, które ze sobą współpracują, a także oprogramowania, które zapewnia przechowywanie i przetwarzanie danych,
- elementy rozległe – czyli sieci teleinformatyczne, które pozwalają na odbieranie, a także wysyłanie danych między systemami informatycznymi, które spełniają rolę urządzeń końcowych.
- sieci teleinformatyczne – są one organizacyjnym i technicznym połączeniem systemów teleinformatycznych[19].

System informatyczny to powiązane z sobą elementy, których funkcją jest przetwarzanie danych przy użyciu techniki komputerowej. Na systemy informatyczne składają się obecnie takie elementy, jak:

- sprzęt - głównie komputery,
- oprogramowanie,
- zasoby osobowe,
- elementy organizacyjne, czyli procedury (procedury organizacyjne) korzystania z systemu informatycznego, instrukcje robocze itp.,
- elementy informacyjne, jak bazy wiedzy — ontologie dziedziny/dziedzin, w których używany jest system informatyczny (na przykład Baza Wiedzy PSP - WIKI).

Reasumując należy stwierdzić, że głównym zadaniem systemów telekomunikacyjnych jest przekazywanie informacji poprzez media komunikacyjne (np. sieci teleinformatyczne, Internet), natomiast systemy informatyczne służą do komputerowego obrabiania pozyskanych informacji i wytworzenia możliwości zautomatyzowania procesów przekazywania danych pomiędzy użytkownikami systemów.

Mając na uwadze, że beneficjentem optymalnego wykorzystania sił i środków krajowego systemu ratowniczo-gaśniczego jest sam obywatel, systemy komunikacyjne i systemy przetwarzania danych w Państwowej Straży Pożarnej pełnią newralgiczną rolę w skutecznej wymianie informacji i co za tym idzie w całości systemu bezpieczeństwa państwa.

Koordynacja i dostęp wszystkich podmiotów współpracujących do danych o prowadzonej akcji ratowniczej zdecydowanie poprawia nie tylko komfort pracy kierującemu działaniami ratowniczymi, ale też dzięki przetwarzaniu informacji przez systemy pozawala na podejmowanie w krótkim czasie trafnych decyzji.

[19] J. Janowski, *Elektroniczny obrót prawny*, Wydawnictwo Wolters Kluwer, Warszawa 2008 r., s. 86.

Ze względu na czysto praktyczne aspekty, systemy funkcjonujące w PSP można podzielić na:

- systemy informatyczne jawne, takie jak:
  - System Wspomagania Decyzji Państwowej Straży Pożarnej (SWD PSP), połączony za pomocą interfejsów komunikacyjnych z Systemem Teleinformatycznym CPR (System Powiadamiania Ratunkowego),
  - system lokalizacji pojazdów pożarniczych na mapie AVL, automatic vehicle location,
  - system wideokonferencyjny PSP,
  - system zasobów elektronicznych, w tym zlokalizowanych w chmurze obliczeniowej PSP, wyposażony w narzędzia informatyczne umożliwiające przeprowadzanie analiz danych o zasobach,
  - system MONITOR-IMGW na potrzeby bieżącego monitorowania sytuacji meteorologicznej i hydrologicznej w kraju przez PSP,
  - system łączności i wymiany informacji w sytuacjach nadzwyczajnych (CECIS) - system wymiany informacji między punktami kontaktowymi właściwymi ds. ratownictwa i ochrony ludności w państwach uczestniczących w Unijnym Mechanizmie Ochrony Ludności - w przypadku Polski jest to Stanowisko Kierowania Komendanta Głównego PSP.
  - W ramach współpracy z Polski w ramach struktur ONZ - platforma internetowa Virtual On-Site Operations Coordination Centre (VOSOCC) oraz Global Disaster Alert and Coordination System (GDACS) – platforma wymiany informacji między ONZ, UE i podmiotami zaangażowanymi w działania międzynarodowe - w przypadku Polski jest to Stanowisko Kierowania Komendanta Głównego PSP
- systemy informatyczne niejawne, zapewniające możliwość bieżącej wymiany informacji niejawnych nie tylko w ramach struktur PSP, ale również np. centrami zarządzania kryzysowego
  - systemy komunikacji radiowej cyfrowej i analogowej, w tym urządzenia końcowe takie jak: radiotelefony stacjonarne (stanowiska kierowania oraz punkty alarmowe jednostek ratowniczo-gaśniczych), radiotelefony przewoźne (pojazdy pożarnicze), radiotelefony nasobne/noszone (urządzenia wykorzystywane przez ratowników),
  - systemy telefoniczne operatora resortowego oraz operatora publicznego, w tym urządzenia końcowe takie jak: telefony stacjonarne (stanowiska kierowania oraz punkty alarmowe jednostek ratowniczo-gaśniczych), telefony mobilne (łączność GSM).

Podstawowym i najważniejszym systemem wymiany informacji na wszystkich szczeblach: od powiatowego przez wojewódzki po krajowy włącznie w Państwowej Straży Pożarnej, a także w ramach całego Systemu Powiadamiania Ratunkowego w Polsce jest Systemu Wspomagania Decyzji Państwowej Straży Pożarnej zwany SWD PSP. Powstał on w 2001 roku i obejmuje swoim zakresem informacyjnym i organizacyjnym główne wydziały Państwowej Straży Pożarnej i jest ustawicznie rozwijany. W ciągu tego okresu powstało kilkadziesiąt wersji, kilka dużych aktualizacji oraz dwie zmiany technologiczne. Pierwsza z nich miała miejsce w 2004 roku, gdy system został wyposażony m.in. w obsługę silnika baz danych Firebird oraz obsługę urządzeń w oparciu o usługi systemowe Windows.[20] W trakcie modernizacji systemu SWD-ST wzbogacił się on także o obsługę różnych urządzeń wspomagających pracę dyspozytorów PSP takich jak moduł mapowy oraz szereg udogodnień i funkcji, które były wprowadzone w wyniku potrzeb użytkowników zarówno od strony technologicznej, jak również od organizacyjnej.

System ten jest typowym interaktywnym systemem komputerowym z rodzaju DSS - Decission Support Systems. Pomaga on decydentom wykorzystać modele i dane w rozwiązywaniu problemów niestrukturalnych, wspierając organizacyjne ich czynności decyzyjne, które powinny ułatwiać modelowanie i rozumienie świata zewnętrznego[21].

Cechami charakterystycznymi takich aplikacji są[22].

- odporność na zakłócenia
- komunikatywność
- precyzja w odtwarzaniu danych ze świata zewnętrznego

Typową architekturę SWD można scharakteryzować wielowymiarowością modelu logicznego oraz fizycznego (m in. tablice wymiarów, tablice faktów, tablice relacji, tablice transformacji), a także ujęciem procesowym.

Istotna funkcjonalność obserwowana współcześnie w SWD to: krótki czas reakcji systemu do wygenerowania raportu, intuicyjność interfejsu, możliwość zagnieżdżania wymiarów w przygotowywaniu raportu tabelarycznego, zdolność rozwijania danych, filtrowanie i sortowanie danych, rotacja, przeobrażenia raportu tabelarycznego w graficzny, projektowanie wykonywalnych raportów, dostęp do danych z wykorzystaniem innych aplikacji (tj. MS Excel, Lotus)[23].

---

[20] https://www.swdst.pl/informacje-o-systemie/ - SWD-ST SYSTEM WSPOMAGANIA DECYZJI ST Informacje o Systemie dostęp na dzień 20.12.20022 r.
[21] Encyklopedia Zarządzania- wersja online, hasło *Organizacja* (dostęp 2022-09-2022)
[22] A. M. Kwiatkowska, *Systemy wspomagania decyzji*, PWN, Warszawa 2007 r. s. 15.
[23] W. Bojar, Rostek K., Knopik L., *Systemy wspomagania decyzji*, PWE, Warszawa 2014 r. s. 20.

W związku z powyższym określony został katalog funkcjonalności SWD PSP, umożliwiający we wszystkich jednostkach organizacyjnych:

- obsługę przyjęcia zgłoszeń i rejestracji zdarzeń,
- alarmowanie i powiadamianie sił i środków krajowego systemu ratowniczo-gaśniczego oraz innych podmiotów współpracujących z systemem,
- dysponowanie sił i środków krajowego systemu ratowniczo-gaśniczego oraz innych podmiotów współpracujących z systemem do działań ratowniczych,
- nadzorowanie i koordynowanie działań ratowniczych,
- sporządzanie dokumentacji z prowadzonych działań,
- wymianę informacji i danych między jednostkami organizacyjnymi Państwowej Straży Pożarnej oraz innymi podmiotami współpracującymi z systemem,
- prowadzenie szczegółowej ewidencji sił i środków Państwowej Straży Pożarnej, Ochotniczej Straży Pożarnej, Zakładowych Straży Pożarnych i Zakładowych Służb Ratowniczych,
- prowadzenie ewidencji dostępnych dla Państwowej Straży Pożarnej sił i środków innych zasobów pochodzących z instytucji i organizacji wspierających Państwową Straż Pożarną,
- współpracę z urządzeniami łączności oraz urządzeniami umożliwiającymi śledzenie pojazdów, nadzór, alarmowanie i powiadamianie sił i środków krajowego systemu ratowniczo-gaśniczego oraz innych podmiotów współpracujących z systemem, a także sterowanie automatyką przemysłową, wykorzystywaną w jednostkach organizacyjnych Państwowej Straży Pożarnej,
- generowanie analiz, raportów, zestawień i statystyk,
- pozyskiwanie danych przestrzennych, udostępnianych za pośrednictwem systemu ,o którym mowa w art. 40 ust. 3 e ustawy – Prawo geodezyjne i kartograficzne, z Głównego Urzędu Geodezji i Kartografii,
- korzystanie z usług danych przestrzennych, udostępnionych za pośrednictwem systemu, o którym mowa w art. 40 ust. 3 e ustawy – Prawo geodezyjne i kartograficzne, z Głównego Urzędu Geodezji i Kartografii,
- wymianę informacji z CPR za pośrednictwem interfejsu komunikacyjnego, którym mowa w art. 13 ust. 2 ustawy o systemie powiadamiania ratunkowego;
- pozyskiwanie i prezentacja danych dotyczących lokalizacji zakończenia sieci, z którego zostało wykonane połączenie do numeru alarmowego, oraz danych dotyczą-

cych abonenta, o których mowa w art. 78 ust. 2 ustawy – Prawo telekomunikacyjne, za pośrednictwem centralnego punktu systemu powiadamiania ratunkowego, o którym mowa w art. 78 ust. 4 pkt 1 ustawy – Prawo telekomunikacyjne, lub przekazanych z CPR;

- współpracę z innymi systemami teleinformatycznymi za pośrednictwem interfejsów zrealizowanych w architekturze otwartej.

Fundamentalnym zadaniem systemu SWD PSP jest wspomaganie pracy strażaków na poziomie stanowisk kierowania PSP, wymiana informacji z Centrami Powiadamiania Ratunkowego, dyspozytorniami PRM oraz stanowiskami kierowania Policji, a także dysponowanie sił i środków jednostek ochrony przeciwpożarowej do działań.

Zgodnie z obowiązującym stanem prawnym tj. Ustawą z dnia 24 sierpnia 1991 r. o ochronie przeciwpożarowej Komendant Główny Państwowej Straży Pożarnej zapewnia funkcjonowanie SWD PSP, stanowiącego system teleinformatyczny wspierający wykonywanie zadań krajowego systemu ratowniczo-gaśniczego przez jednostki organizacyjne Państwowej Straży Pożarnej oraz przyjmowanie zgłoszeń alarmowych z centrów powiadamiania ratunkowego, o których mowa w ustawie z dnia 22 listopada 2013 r. o systemie powiadamiania ratunkowego.

Utrzymanie, rozbudowa i modyfikacje SWD PSP są finansowane z budżetu państwa z części, której dysponentem jest minister właściwy do spraw wewnętrznych oraz z części, których dysponentami są właściwi wojewodowie.

Ponadto Minister właściwy do spraw wewnętrznych określił, w drodze rozporządzenia z dnia 30 kwietnia 2021 r. w sprawie Systemu Wspomagania Decyzji Państwowej Straży Pożarnej: minimalny zbiór funkcjonalności SWD PSP, w tym sposób funkcjonowania systemu w sytuacjach awaryjnych, a także sposób przydzielania, zawieszania oraz uchylania dostępu do tego systemu użytkownikom Państwowej Straży Pożarnej oraz jednostkom ochrony przeciwpożarowej, uwzględniając potrzebę zapewnienia optymalnego poziomu współpracy między tym systemem a systemem teleinformatycznym systemu powiadamiania ratunkowego.

Celem zagwarantowania zwiększenia niezawodności funkcjonowania SWD PSP m.in. w zakresie interoperacyjności, zapewnienia ciągłego monitorowania jego stanu, szybkiego reagowania i usuwania ewentualnych awarii w możliwie najkrótszym czasie, zwłaszcza pod kątem współpracy z systemem teleinformatycznym wykorzystywanym

w CPR, Komendant Główny PSP sprecyzował dla SWD PSP gwarancję świadczenia usług – Service Level Agreement (SLA), na poziomie 98,5 % w ciągu roku.

Ponadto Komendant Główny PSP określił sposób szczegółowy wymagania, jakie powinny być spełnione przy wypełnianiu w systemie SWD PSP formatek karty zdarzenia oraz informacji ze zdarzenia wdrażając Zasady ewidencjonowania zdarzeń w Systemie Wspomagania Decyzji Państwowej Straży Pożarnej.

Dokument składa się z czterech części:

- pierwsza i druga określają szczegółowe zasady prowadzenia dokumentacji zdarzeń, czasookres jej sporządzania, przesyłania, tryb kontroli poprawności, wprowadzania zmian w informacji ze zdarzenia przez stanowiska kierowania komendanta powiatowego/miejskiego, komendanta wojewódzkiego Państwowej Straży Pożarnej oraz osoby odpowiedzialne za sporządzanie poszczególnych elementów dokumentacji,
- trzecia część opracowania określa zasady sporządzania informacji ze zdarzenia,
- czwarta - wybrane problemy w formie pytań i odpowiedzi.

Systemem, stricte powiązanym z SWD PSP i wspomagającym oraz ułatwiającym pracę dyżurnego, a także dającym mu możliwość koordynowania czasu dojazdu jednostek na miejsce zdarzenia, zmianę statusów zgłoszenia czy lokalizację pojazdów na mapie jest system AVL, automatic vehicle location, czyli automatyczne śledzenie pojazdów.

Kolejnym newralgicznym systemem i narzędziem do wymiany informacji w ramach Państwowej Straży Pożarnej jest system radiowy. Jest to zespół niezbędnego wyposażenia i urządzeń do prowadzenia niezawodnej łączności. Aktualnie to nie tylko łączność stacjonarna czy autonomiczne systemy komunikacji radiowej. To systemy integrujące wszystkie posiadane środki, niezależnie analogowe czy cyfrowe, mobilne czy stacjonarne. Również takie, które ułatwią lub umożliwią bezpośredni kontakt z abonentami innych służb i instytucji.

System radiowy należy rozumieć jako system łączności radiowej i telefonicznej, służący do wymiany informacji głosowych, tonowych oraz danych, wraz z systemem rejestracji i archiwizacji całej korespondencji.

Wdrożenie takiego systemu oznacza m.in.:

- obsługę wszystkich połączeń przychodzących i wychodzących — radiotelefonicznych (analogowych i cyfrowych) i telefonicznych — przy użyciu jednego terminala,
- rejestrację i archiwizację całej korespondencji,
- kolejkowanie połączeń przychodzących,

- integrację ze środkami łączności innych służb,
- dużą ergonomię pracy i elastyczną rozbudowę,
- sterowanie automatyką budynkową z jednego stanowiska.

Intuicyjna obsługa oraz indywidualnie tworzone profile użytkownika ułatwiają pracę dyżurnemu, a zwierzchnikowi jej analizę.

Przy rozbudowie systemu zakłada się m.in. wykorzystanie posiadanych obecnie przez jednostki Państwowej Straży Pożarnej środków łączności radiowej i telefonicznej – brak konieczności wymiany używanego aktualnie sprzętu oraz integrację z urządzeniami automatyki w budynkach.

Fundamentalnym zadaniem systemu radiowego jest zapewnienie łączności pomiędzy stacją stałą stanowiska kierowania, a stacjami pracującymi w tej sieci, ze szczególnym uwzględnieniem bezpośredniego kontaktu z Kierującym Działaniem Ratowniczym.
Zgodnie z obowiązującym stanem prawnym tj. Rozkazem Nr 8 Komendanta Głównego Państwowej Straży Pożarnej z dnia 5 kwietnia 2019 r. w sprawie wprowadzenia nowych zasad organizacji łączności radiowej[24] Państwowa Straż Pożarna dla realizacji łączności radiowej wykorzystuje częstotliwości z pasma UKF136-174 MHz (w modulacji F3E oraz FXD FXE), będącego w dyspozycji resortu spraw wewnętrznych i w paśmie TETRA 380-400 MHz.

Pasmo UKF zostało podzielone na kanały radiowe z odstępem międzykanałowym 12,5 kHz. Kierując się wymaganiami taktyczno-operacyjnymi służby, strukturą organizacyjną, możliwościami technicznymi i optymalnym wykorzystaniem przydzielonego pasma częstotliwości, przyjęto następującą strukturę sieci radiowych ultrakrótkofalowych:

- Krajowa Sieć Współdziałania i Alarmowania (KSW) - sieć, pracująca w oparciu o ogólnopolski kanał radiowy, służąca do alarmowania, wywołania, powiadomienia i współpracy w razie zaistnienia ważnych przyczyn. Podstawową zasadą sieci jest zapewnienie dwustronnej łączności pomiędzy sąsiadującymi stacjami nasłuchowymi, a także pomiędzy stacjami przewoźnymi i stacjami nasłuchowymi, w zasięgu których znajdują się te stacje przewoźne. Dodatkowo służy siłom i środkom kierowanym do działań z innych powiatów/województw do zgłaszania swojego przyjazdu do właściwego dla miejsca działań SKKP/SKKM lub koordynacji przyjęcia pojazdów przez

[24] Dziennik Urzędowy Komendy Głównej Państwowej Straży Pożarnej z 2019 roku Poz. 7.

PPSiŚ. Nasłuch Krajowej Sieci Współdziałania i Alarmowania prowadzą wszystkie stanowiska kierowania.

- Sieć Wojewódzka (PW) - sieć radiowa o stałym obszarze pracy, obejmująca zasięgiem radiowym obszar województwa. Służy SKKW do koordynacji działań na szczeblu Stanowisk Kierowania PSP, współdziałania pomiędzy sąsiednimi SKKP/SKKM oraz do utrzymywania łączności pomiędzy stacją stałą SKKW, a stacjami ruchomymi będącymi w dyspozycji KW PSP.
- Sieć Powiatowa (PR) - sieć radiowa o stałym obszarze pracy, obejmująca zasięgiem radiowym obszar powiatu lub rejon działania KP/KM PSP. Zapewnia łączność pomiędzy stacją stałą SKKP/SKKM, a stacjami pracującymi w tej sieci. Sieć Powiatowa powinna gwarantować pokrycie zasięgiem radiowym obszaru powiatu dla relacji: stacja stała SKKP/SKKM - stacja przewoźna.
- Sieć Szkolna (KS) - sieć radiowa o stałym obszarze pracy. Umożliwia łączność pomiędzy stacją stałą Szkoły, a innymi stacjami będącymi w dyspozycji szkoły.
- Sieć Szkolno-Dydaktyczna (KSD) - ruchoma sieć radiowa o stałym obszarze pracy, przeznaczona dla potrzeb szkolnych i dydaktycznych Szkół PSP w ich lokalizacjach.
- Sieć Dydaktyczno-Szkoleniowa (KWOS) - ruchoma sieć radiowa o stałym obszarze pracy przeznaczona dla potrzeb dydaktyczno-szkoleniowych Wojewódzkich Ośrodków Szkolenia w ich lokalizacjach.
- Sieć Komendy Głównej (PG) - sieć o stałym obszarze pracy, obejmująca zasięgiem obszar Warszawy, zapewniająca łączność pomiędzy stacją stałą, a stacjami ruchomymi będącymi w dyspozycji KG PSP.
- Operacyjny Kierunek Radiowy (KO) - sposób organizacji łączności uruchamianej doraźnie, zapewniający bezpośrednią łączność pomiędzy SKKP/SKKM, a sztabem KDR.
- Sieć Dowodzenia i Współdziałania (KDW) - sieć o zmiennym obszarze pracy, funkcjonująca na bazie stacji ruchomych, uruchamiana doraźnie podczas akcji ratowniczo-gaśniczych. Sieć KDW służy zapewnieniu łączności dowodzenia i współdziałania pomiędzy siłami ratowniczymi własnymi oraz współdziałającymi.
- Sieć Ratowniczo-Gaśnicza (KRG) - sieć o zmiennym obszarze pracy funkcjonująca na bazie stacji ruchomych, przeznaczona dla potrzeb łączności w miejscu prowadzenia akcji ratowniczo-gaśniczej.

- Krajowa Sieć Współdziałania ze Statkami Powietrznymi (KSWL) - sieć radiowa ruchoma o zmiennym obszarze pracy, uruchamiana doraźnie na terenie kraju z zastosowaniem stacji stacjonarnych, przewoźnych i noszonych. Sieć KSWL zapewnia łączność pomiędzy jednostkami PSP, a statkami powietrznymi, biorącymi udział w akcjach ratowniczych.
- Radiowa Sieć Retransmisyjna (RSR) - sieć ruchoma o zmiennym obszarze pracy, wykorzystująca mobilną stację retransmisyjną oraz stacje radiowe przewoźne i noszone na terenie całego kraju, wykorzystywana w celu zwiększenia zasięgu łączności radiowej na potrzeby KDR.

Ponadto newralgicznymi sieciami radiowymi do alarmowania lub współdziałania ze służbami, instytucjami a w szczególności Ochotniczymi Strażami Pożarnymi są:

- Sieć Alarmowa (PA) - sieć radiowa o stałym obszarze pracy, umożliwiająca nawiązanie łączności pomiędzy stacją SKKP/SKKM, a stacjami podległymi, zainstalowanymi w jednostkach ochrony przeciwpożarowej. Sieć służąca do alarmowania jednostek OSP do działań poprzez uruchamianie systemów alarmowania OSP.
- Sieci Współdziałania z innymi podmiotami - sieci radiowe, których dysponentami są inne jednostki/organizacje/służby (sieć współdziałania MSWiA-B112, ogólnopolska sieć służby zdrowia – PRM itp.).
- Krajowa Sieć Współpracy z Harcerzami (KSH) - sieć ruchoma typu otwartego o zmiennym obszarze pracy, przeznaczona dla zapewnienia doraźnej łączności w lokalizacji pobytu uczestników obozów harcerskich, w sytuacji wymagającej podjęcia działań ratowniczych ze strony jednostek ochrony przeciwpożarowej (PSP, OSP) lub do zapewnienia dwustronnej łączności pomiędzy stacjami radiowymi będącymi na wyposażeniu komendantur obozów harcerskich, a stacjami nasłuchowymi stanowisk kierowania PSP, w zasięgu których będą znajdować się te stacje.
- Pasmo TETRA - Państwowa Straż Pożarna dla realizacji łączności radiowej w systemie TETRA wykorzystuje częstotliwości w paśmie 380-400 MHz, będące w dyspozycji Ministerstwa Spraw Wewnętrznych i Administracji. Operatorem Systemu TETRA jest Policja.
- Kierując się wymaganiami taktyczno-operacyjnymi służby, strukturą organizacyjną, możliwościami technicznymi i optymalnym wykorzystaniem przydzielonego pasma częstotliwości, przyjęto następującą strukturę grup radiowych w standardzie TETRA:

- Grupa Wojewódzka (GPW) - grupa obejmująca zasięgiem radiowym obszar województwa. Służy SKKW do koordynacji działań na szczeblu SKKP/SKKM, współdziałania pomiędzy sąsiednimi stanowiskami kierowania oraz do utrzymywania łączności pomiędzy stacją stałą SKKW, a stacjami ruchomymi będącymi w dyspozycji KW PSP.
- Grupa Powiatowa (GPR) - grupa obejmująca zasięgiem radiowym obszar powiatu lub rejon działania KP/KM PSP. Zapewnia łączność pomiędzy stacją stałą Stanowiska Kierowania Komendanta Miejskiego/Powiatowego (SKKM/SKKP), a stacjami pracującymi w tej grupie.
- Grupa Szkolna (GKS) - grupa radiowa mogąca obejmować zasięgiem radiowym obszar powiatu oraz województwa właściwy dla lokalizacji Szkoły. Umożliwia łączność pomiędzy stacją stałą Szkoły, a innymi stacjami będącymi w dyspozycji Szkoły.
- Grupa Dowodzenia i Współdziałania (GKDW) – grupa uruchamiana doraźnie podczas akcji ratowniczo-gaśniczych, służąca zapewnieniu łączności dowodzenia i współdziałania pomiędzy siłami ratowniczymi.
- Grupa Ratowniczo-Gaśnicza (GKRG) - grupa o stałym obszarze pracy, przeznaczona dla potrzeb łączności w miejscu prowadzenia akcji ratowniczo-gaśniczej.
- Grupa Współdziałania z innymi służbami - grupa przeznaczona na potrzeby współdziałania służb biorących udział w działaniach ratowniczo-gaśniczych, o ile dana służba wyposażona została w terminale systemu TETRA.

Innym kluczowym systemem wymiany informacji w ramach Państwowej Straży Pożarnej jest System Alarmowania, przez Państwową Straż Pożarną, Ochotniczych Straży Pożarnych włączonych do krajowego systemu ratowniczo-gaśniczego. Fundamentalnym zadaniem tego systemu jest zdalne uruchamianie syren alarmowych jednostek OSP na terenie całego powiatu, przez dyżurnego SK KP (KM) PSP. Wszystkie jednostki ochrony przeciwpożarowej powoływane są w celu ratowania życia, mienia oraz środowiska - dotyczy to również jednostek ochotniczych straży pożarnych, których powiadamianie wymaga zorganizowania sprawnego systemu alarmowania.

Zgodnie z obowiązującym stanem prawnym tj. Rozporządzeniem Ministra Spraw Wewnętrznych z dnia 15 września 2014 roku w sprawie zakresu, szczegółowych warunków włączania jednostek ochrony przeciwpożarowej do krajowego systemu ratowniczo-gaśniczego do ksrg mogą być włączane jednostki ochrony przeciwpożarowej, których siły i środki są przewidziane do użycia w powiatowym lub wojewódzkim planie ratowniczym,

które zostały uwzględnione w zbiorczym planie sieci podmiotów systemu oraz posiadają oprócz co najmniej jednego średniego lub ciężkiego samochodu ratowniczo-gaśniczego, co najmniej 12 wyszkolonych ratowników oraz posiadają skuteczny system łączności powiadamiania i alarmowania (tj. System Alarmowania OSP), a także urządzenia łączności w sieci radiowej systemu na potrzeby działań ratowniczych;

Ponadto unormowane jest to w dodatkowych przepisach:

- art. 21b pkt 4 ustawy z dnia 24 sierpnia 1991 r. o ochronie przeciwpożarowej: „Do zadań własnych powiatu w zakresie ochrony przeciwpożarowej należy: organizowanie systemu łączności, alarmowania i współdziałania między podmiotami uczestniczącymi w działaniach ratowniczych na obszarze powiatu”;
- § 4 ust. 1 pkt 7 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 17 września 2021 r. w sprawie szczegółowej organizacji krajowego systemu ratowniczo-gaśniczego: „Organizacja funkcjonowania ksrg przez komendanta powiatowego (miejskiego) Państwowej Straży Pożarnej, na obszarze powiatu, obejmuje w szczególności: ustalenie zasad powiadamiania, alarmowania i współdziałania podmiotów podczas działań ratowniczych”;
- § 2 ust. 1 pkt 1 lit. c rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 15 września 2014 r. w sprawie zakresu, szczegółowych warunków i trybu włączania jednostek ochrony przeciwpożarowej do krajowego systemu ratowniczo-gaśniczego: „Do systemu może zostać włączona jednostka, która posiada skuteczny system łączności powiadamiania i alarmowania”.

W przypadku jednostek OSP włączonych do krajowego systemu ratowniczo-gaśniczego syreny alarmowe uruchamianie są zdalnie ze stanowisk kierowania komend powiatowych (miejskich) PSP, w ramach systemów selektywnego alarmowania. Przyjęte i funkcjonujące aktualnie rozwiązania są sprawdzonym i efektywnym sposobem alarmowania strażaków ochotników, niemniej jednak dopuszczalne jest zastosowanie alternatywnego sposobu alarmowania jednostek ochotniczych straży pożarnych pod warunkiem, że będzie on skuteczny i nie doprowadzi do obniżenia mobilności jednostki. Jednakże, należy pamiętać iż wszelkie zmiany spowodują konieczność poniesienia dodatkowych kosztów przez władze gminy, które zgodnie z zapisami wyżej wymienionej ustawy o ochronie przeciwpożarowej ponoszą koszty wyposażenia, utrzymania, wyszkolenia i zapewnienia gotowości bojowej ochotniczej straży pożarnej.

W latach 90 jedynym systemem alarmowania jednostek OSP przez stanowiska kierowania PSP poziomu powiatowego i miejskiego były wyłącznie syreny alarmowe. Dyspozytor danej komendy PSP, gdy otrzymywał informację o zdarzeniu w danej miejscowości dzwonił do osoby, która była wskazana w danym OSP do alarmowania, ta osoba udawała się do remizy i ręcznie uruchamiała syrenę. Obecne rozwiązania techniczne pozwalają realizować alarmowanie jednostek OSP wielotorowo, choć wykorzystanie syren alarmowych w dalszym ciągu stanowi jego podstawowy element.

Teraz w przypadku zagrożenia dana OSP jest dysponowana ze stanowiska kierowania komendanta powiatowego za pomocą sygnału radiowego o odpowiedniej częstotliwości, który jest przesyłany do remizy i uruchamia syrenę. Dźwięk trwa około 30 sekund, z 10-sekundową przerwą, powtarzany jest dwukrotnie, także w ciągu 2 minut jest ten sygnał wyemitowany dla każdej jednostki, która jest w selektywnym alarmowaniu. Równolegle dźwiękiem syreny wzywającym druhów OSP, otrzymują oni powiadomienie SMS-owe. Selektywne alarmowanie ułatwiło pracę dyspozytorowi PSP, a przede wszystkim bardzo skróciło czas alarmowania. Szybciej można zebrać druhów w remizie, a co za tym idzie wyjechać do zdarzenia.

Wielowariantowość alarmowania tj.: syreny alarmowe, pagery (które w przypadku części strażaków nadal funkcjonują) i powiadomienia otrzymywane przez strażaków w tym samym czasie na telefon komórkowy zmniejszają prawdopodobieństwo braku powiadomienia ratowników OSP, jeżeli któryś ze środków technicznych zawiedzie.

Elementem bezpieczeństwa wewnętrznego jest także monitoring systemów sygnalizacji pożarowej, do którego należy analiza stanu zagrożenia, alarmowania o możliwości realnego zagrożenia, ostrzeganie pracowników, włączanie systemów zabezpieczających, alarmowanie sił ratowniczych, ostrzeganie ludności itp.[25].

Nadrzędnym zadaniem systemu jest przesłanie z potwierdzeniem, w sposób automatyczny alarmu pożarowego i sygnałów uszkodzeniowych do odpowiednich alarmowych centrów odbiorczych. Przesłanie alarmu pożarowego musi odbywać się bez udziału człowieka do obiektu z ciągłą obsługą, z którego dysponowane są siły i środki Państwowej Straży Pożarnej, wskazanego przez właściwego miejscowo komendanta powiatowego/ miejskiego Państwowej Straży Pożarnej, gdzie zamontowana jest stacja odbiorcza alarmów pożarowych (SOAP). Sygnały uszkodzeniowe kierowane są automatycznie do stacji odbiorczej sygnałów uszkodzeniowych operatora systemu monitoringu pożarowego.

[25] Krajowy System Ratowniczo-Gaśniczy, *Ratownictwo chemiczno-ekologiczne*, Warszawa 1983 r., s. 52;

Zgodnie z obowiązującym stanem prawnym tj. Rozporządzeniem Ministra Spraw Wewnętrznych i Administracji z dnia 7 czerwca 2010 r. w sprawie ochrony przeciwpożarowej budynków, innych obiektów budowlanych i terenów stosowanie systemu sygnalizacji pożarowej, obejmującego urządzenia sygnalizacyjno-alarmowe, służące do samoczynnego wykrywania i przekazywania informacji o pożarze, a także urządzenia odbiorcze alarmów pożarowych i urządzenia odbiorcze sygnałów uszkodzeniowych, jest wymagane w:

- budynkach handlowych lub wystawowych:
  - jednokondygnacyjnych o powierzchni strefy pożarowej powyżej 5 000 $m^{2,}$
  - wielokondygnacyjnych o powierzchni strefy pożarowej powyżej 2 500 m^2,
- teatrach o liczbie miejsc powyżej 300;
- kinach o liczbie miejsc powyżej 600;
- budynkach o liczbie miejsc służących celom gastronomicznym powyżej 300;
- salach widowiskowych i sportowych o liczbie miejsc powyżej 1 500;
- szpitalach, z wyjątkiem psychiatrycznych oraz w sanatoriach - o liczbie łóżek powyżej 200 w budynku;
- szpitalach psychiatrycznych o liczbie łóżek powyżej 100 w budynku;
- domach pomocy społecznej i ośrodkach rehabilitacji dla osób niepełnosprawnych o liczbie łóżek powyżej 100 w budynku;
- zakładach pracy zatrudniających powyżej 100 osób niepełnosprawnych w budynku;
- budynkach użyteczności publicznej wysokich i wysokościowych;
- budynkach zamieszkania zbiorowego, w których przewidywany okres pobytu tych samych osób przekracza trzy doby, o liczbie miejsc noclegowych powyżej 200,
- budynkach zamieszkania zbiorowego niewymienionych w pkt powyżej, o liczbie miejsc noclegowych powyżej 50;
- archiwach wyznaczonych przez Naczelnego Dyrektora Archiwów Państwowych;
- muzeach oraz zabytkach budowlanych, wyznaczonych przez Generalnego Konserwatora Zabytków w uzgodnieniu z Komendantem Głównym Państwowej Straży Pożarnej;
- ośrodkach elektronicznego przetwarzania danych o zasięgu krajowym, wojewódzkim i w urzędach obsługujących organy administracji rządowej;
- centralach telefonicznych o pojemności powyżej 10 000 numerów i centralach telefonicznych tranzytowych o pojemności 5 000 10 000 numerów, o znaczeniu miejscowym lub regionalnym;

- garażach podziemnych, w których strefa pożarowa przekracza 1 500 m^2 lub obejmujących więcej niż jedną kondygnację podziemną;
- stacjach metra i stacjach kolei podziemnych;
- dworcach i portach, przeznaczonych do jednoczesnego przebywania powyżej 500 osób;
- bankach, w których strefa pożarowa zawierająca salę operacyjną ma powierzchnię przekraczającą 500 m^2,
- bibliotekach, których zbiory w całości lub w części tworzą narodowy zasób biblioteczny.

Wymagania, powyższe nie dotyczą budynków, które są zlokalizowane na terenach zamkniętych służących obronności państwa oraz budynków zakwaterowania osadzonych, które zlokalizowane są na terenach zakładów karnych i aresztów śledczych.

Ponadto w Komendzie Głównej opracowano Zasady monitoringu sił i środków ksrg celem jednoznacznego określenia poziomu dostępności SIS ksrg do natychmiastowego użycia w działania ratowniczych w kraju jak i poza jego granicami. Zasady określają zadania do realizacji dla stanowisk kierowania PSP (wszystkich poziomów: krajowego, wojewódzkiego, powiatowego/miejskiego) oraz szkolnych stanowisk kierowania, a w szczególności częstotliwość i rodzaj przekazywanych informacji do Stanowiska Kierowania Komendanta Głównego PSP. Monitoring ten realizowany jest na bieżąco przez wszystkie stanowiska kierowania PSP każdego poziomu w oparciu o funkcjonalności SWD PSP.

Monitoring poziomu dostępności specjalistycznych grup ratowniczych realizowany jest w oparciu o zestawienia tabelaryczne przekazywane pomiędzy stanowiskami kierowania PSP w oparciu o funkcjonujące rozwiązania teleinformatyczne. W ramach codziennego monitoringu sprawdzana jest deklarowana gotowości poszczególnych grup w stosunku do poziomów przyjętych w Rozkazie Komendanta Głównego PSP w sprawie organizacji centralnego odwodu operacyjnego krajowego systemu ratowniczego-gaśniczego.

Stanowiska kierowania komendantów powiatowych (miejskich) PSP, na terenie których utworzone zostały specjalistyczne grupy ratownicze, codziennie rano przekazują informacje do stanowisk kierowania komendantów wojewódzkich PSP o gotowości poszczególnych grup. Zestawienia za województwa przekazywane są do Stanowiska Kierowania Komendanta Głównego PSP, które sporządza zestawienie zbiorcze za cały kraj.

Właściwe stanowiska kierowania komendantów wojewódzkich PSP przekazują do Stanowiska Kierowania Komendanta Głównego PSP w trybie miesięcznym informację o gotowości do wyjazdu danego modułu w momencie rozpoczęcia miesięcznego dyżuru. Służba dyżurna SK KG PSP weryfikuje otrzymane dane z "Planem najbardziej prawdopodobnego dysponowania modułów ratowniczych" na dany rok kalendarzowy (dokument opracowywany w Biurze Planowania Operacyjnego KG PSP).

Funkcjonuje także system monitoringu ilości środka pianotwórczego. Informacje ze stanowisk kierowania komendantów wojewódzkich PSP przekazywane są do Stanowiska Kierowania Komendanta Głównego PSP w trybie miesięcznym oraz na bieżąco w przypadku zmniejszenia zapasu środka pianotwórczego poniżej 60% uzgodnionego z Komendą Główną PSP. Stanowisko Kierowania Komendanta Głównego PSP, które sporządza zestawienie zbiorcze za cały kraj.

Ponadto uwzględnić należy monitoring całodobowych racji żywnościowych. Informacje o stanie ilościowym oraz terminie przydatności całodobowych racji żywnościowych przekazywane są do Stanowiska Kierowania Komendanta Głównego PSP przez szkolne stanowiska kierowania w trybie miesięcznym na każdy pierwszy dzień roboczy kolejnego miesiąca oraz w dni ich ewentualnego zadysponowania. Stanowisko Kierowania Komendanta Głównego PSP, które sporządza zestawienie zbiorcze za cały kraj.

Wymiana informacji PSP z Systemem Powiadamiania Ratunkowego następuje zgodnie z Ustawą z dnia 22 listopada 2013 r. o systemie powiadamiania ratunkowego, gdzie określone zostały ramy oraz mechanizmy obsługi zgłoszenia alarmowego (kierowanego do numerów alarmowych 112, 997, 998 i 999). W Polsce utworzony został jednolity system, składający się z 17 centrów powiadamiania ratunkowego (16 CPR do obsługi każdego województwa oraz dodatkowo do obsługi m. st. Warszawa), umożliwiający wymianę informacji, w tym przekazanie zgłoszenia alarmowego w celu zaangażowania właściwych zasobów ratowniczych.

System Powiadamiania Ratunkowego został przewidziany do pracy w tym wymiany informacji pomiędzy PSP i CPR, a także innymi służbami w dwóch trybach:

- podstawowy tryb pracy systemu (za pośrednictwem systemu teleinformatycznego – formatki) – funkcjonującym zgodnie z „Procedurą obsługi zgłoszeń alarmowych za pośrednictwem Systemu Teleinformatycznego CPR (STCPR)" – formatka CPR,
- redundantny tryb pracy systemu (za pośrednictwem systemu telefonicznego – połączenia głosowego) – uruchamianym w przypadku braku możliwości przekazania zda-

rzenia do dyspozytora/dyżurnego służby, za pośrednictwem STCPR, stosuje się „Szczegółowe procedury do obsługi zgłoszeń alarmowych w modelu telefonicznym" – połączenie głosowe, telefoniczne.

Celem realizacji powyższego modelu i zapewnienia możliwości obsługi obydwu trybów tj., zbudowana została wydzielona sieć teleinformatyczna na potrzeby obsługi numerów alarmowych (OST 112), łączącą centra powiadamiania ratunkowego, jednostki organizacyjne Policji, Państwowej Straży Pożarnej, dysponentów zespołów ratownictwa medycznego, służąca do wymiany danych dotyczących zgłoszenia alarmowego. W ramach projektu budowy OST 112 przewidziano i wdrożono przyłącza podstawowe oraz zapasowe. Do obsługi jednostek organizacyjnych PSP na poszczególnych trzech poziomach: powiatowym, wojewódzkim i krajowym zapewniono dla:

- poziomu powiatu tj.: 335 komend powiatowych (miejskich) PSP – 335 łączy podstawowych i 335 łączy rezerwowych,
- poziomu województwa tj. 16 komend wojewódzkich PSP – 16 łączy podstawowych i 16 łączy rezerwowych,
- poziomu kraju (poziom centralny) tj.: Komendy Głównej PSP – 1 łącze podstawowe i 1 łącze rezerwowe.

Do realizacji obsługi zgłoszeń alarmowych za pośrednictwem systemu teleinformatycznego zapewniono możliwość wymiany formatek pomiędzy system CPR (System Powiadamiania Ratunkowego), a systemami służb, w tym także system organizowanym przez PSP, tj. System Wspomagania Decyzji Państwowej Straży Pożarnej – SWD PSP. Celem kompatybilnej współpracy, a także zachowaniem spójności i tożsamości ww. systemów, zbudowano interfejsy komunikacyjne systemów teleinformatycznych, umożliwiające dostęp do danych przestrzennych, informacji dotyczących lokalizacji zakończenia sieci, z którego zostało wykonane połączenie na numer alarmowy oraz danych dotyczących abonenta.

Mając na uwadze najwyższe standardy w zakresie udzielenia jak najszybszej pomocy osobie jej potrzebującej system powiadamiania ratunkowego działa z zastosowaniem zasady wzajemnej zastępowalności centrów w razie miejscowej awarii systemu teleinformatycznego bądź jego przeciążenia.

Na potrzeby centrum zapewniono w szczególności:

- urządzenia zasilania awaryjnego dla urządzeń teleinformatycznych i innych urządzeń elektrycznych;

- urządzenia techniczne i środki łączności oraz systemy teleinformatyczne zapewniające realizację zadań systemu powiadamiania ratunkowego w sposób efektywny, z zachowaniem ciągłości jego działania i wymiany informacji oraz możliwości pracy, szczególnie w przypadku braku zasilania zewnętrznego lub uszkodzenia systemów teleinformatycznych.

Sposób obsługi zgłoszenia, będącego zgłoszeniem alarmowym (system wymiany informacji w relacjach PSP – CPR) wygląda następująco. Operator Numeru Alarmowego (ONA), Centrum Powiadamiania Ratunkowego, przyjmuje zgłoszenia będące zgłoszeniami alarmowymi typu:

- wiadomość głosowa (połączenie telefoniczne na numer alarmowy),
- wiadomość eCall,
- wiadomość SMS,

i równocześnie z przeprowadzaną rozmową z osobą zgłaszającą, ONA wypełnia oraz zapisuje zebrane dane w formatce w ST CPR. W tym momencie powstaje zarejestrowanie zgłoszenia alarmowego w systemie teleinformatycznym.

Zadaniem tego etapu jest uzyskanie informacji o:

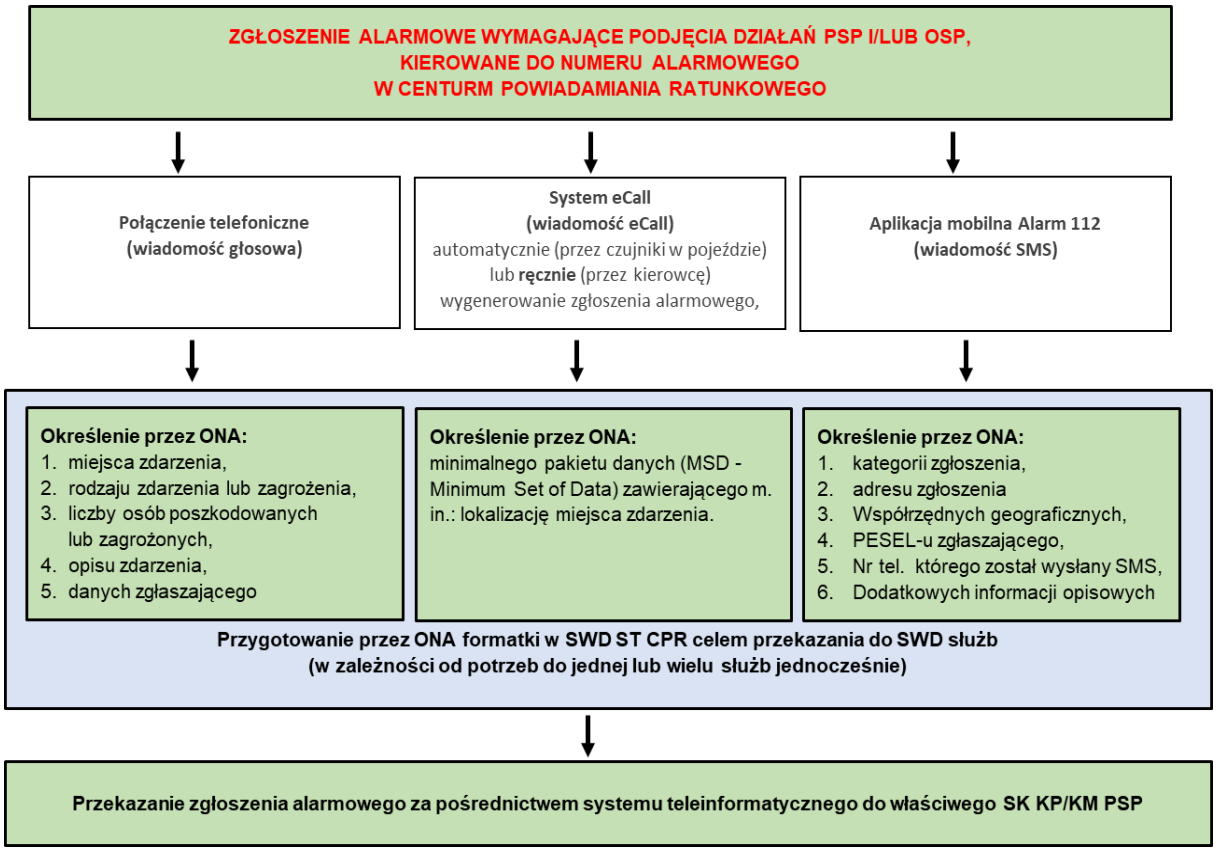
a) rodzaju zdarzenia lub zagrożenia,
b) miejscu zdarzenia lub zagrożenia – w przypadku wątpliwości związanych z ustaleniem dokładnego miejsca zdarzenia lub zagrożenia należy uzyskać dodatkowe informacje dotyczące miejsca zdarzenia lub zagrożenia, umożliwiające szybkie dotarcie właściwych podmiotów ratowniczych,
c) liczbie osób poszkodowanych lub będących w stanie nagłego zagrożenia zdrowotnego,
d) danych osoby zgłaszającej obejmujących imię, nazwisko oraz numer telefonu, jeżeli je podała, na wypadek konieczności uzyskania dodatkowych informacji o zdarzeniu lub zagrożeniu,
e) innych istotnych okolicznościach zdarzenia lub zagrożenia, umożliwiających podjęcie czynności przez podmioty ratownicze;
f) potwierdzenie osobie zgłaszającej przyjęcia zgłoszenia alarmowego;
g) przekazanie zgłoszenia alarmowego za pośrednictwem systemu teleinformatycznego właściwemu dyspozytorowi lub dyspozytorom podmiotów ratowniczych, których numery są obsługiwane w ramach systemu powiadamiania ratunkowego;

h) poinformowanie osoby zgłaszającej o przekazaniu zgłoszenia alarmowego do odpowiedniego podmiotu ratowniczego lub podmiotów ratowniczych zgodnie z kwalifikacją rodzaju zdarzenia lub zagrożenia;
i) odbiór potwierdzenia przyjęcia zgłoszenia alarmowego przez właściwego dyspozytora;
j) podjęcie niezbędnych czynności zmierzających do spowodowania przyjęcia zgłoszenia alarmowego w przypadku braku potwierdzenia odbioru zgłoszenia alarmowego przez właściwego dyspozytora

Szczegółowy katalog zdarzeń i odpowiednich do nich pytań, które ONA zadaje zgłaszającemu, zgłoszenie alarmowe, szczegółowe procedury obsługi zgłoszeń alarmowych, a także procedury przekazania zgłoszenia w sytuacji awaryjnej są opracowywane i aktualizowane przez ministra właściwego do spraw administracji, we współpracy z wojewodami, Policją, Państwową Strażą Pożarną i podmiotami ratowniczymi, których numery są obsługiwane w ramach systemu powiadamiania ratunkowego.

Zgłoszenie alarmowe przekazywane do właściwego dyspozytora w ramach systemu powiadamiania ratunkowego zawiera:

- unikatowy identyfikator zgłoszenia alarmowego;
- datę i godzinę przyjęcia zgłoszenia alarmowego;
- informację o miejscu zdarzenia lub zagrożenia, określającą to miejsce w sposób umożliwiający szybkie dotarcie właściwych podmiotów ratowniczych;
- opis zdarzenia lub zagrożenia, w tym liczbę osób poszkodowanych lub będących w stanie nagłego zagrożenia zdrowotnego;
- identyfikator operatora numerów alarmowych, który przyjął zgłoszenie alarmowe;
- informację o podmiocie lub podmiotach ratowniczych, do których skierowano zgłoszenie alarmowe;
- rodzaj zdarzenia lub zagrożenia według katalogu zdarzeń, o którym mowa powyżej;
- informacje dotyczące lokalizacji zakończenia sieci, z którego zostało wykonane połączenie do numeru alarmowego;
- odnośnik do dokumentu elektronicznego zawierającego treść oryginalnego zgłoszenia alarmowego.



Źródło: Opracowanie własne.

Rysunek 3-2

Przebieg zgłoszenia alarmowego przekazywanego do systemu powiadamiania ratunkowego.

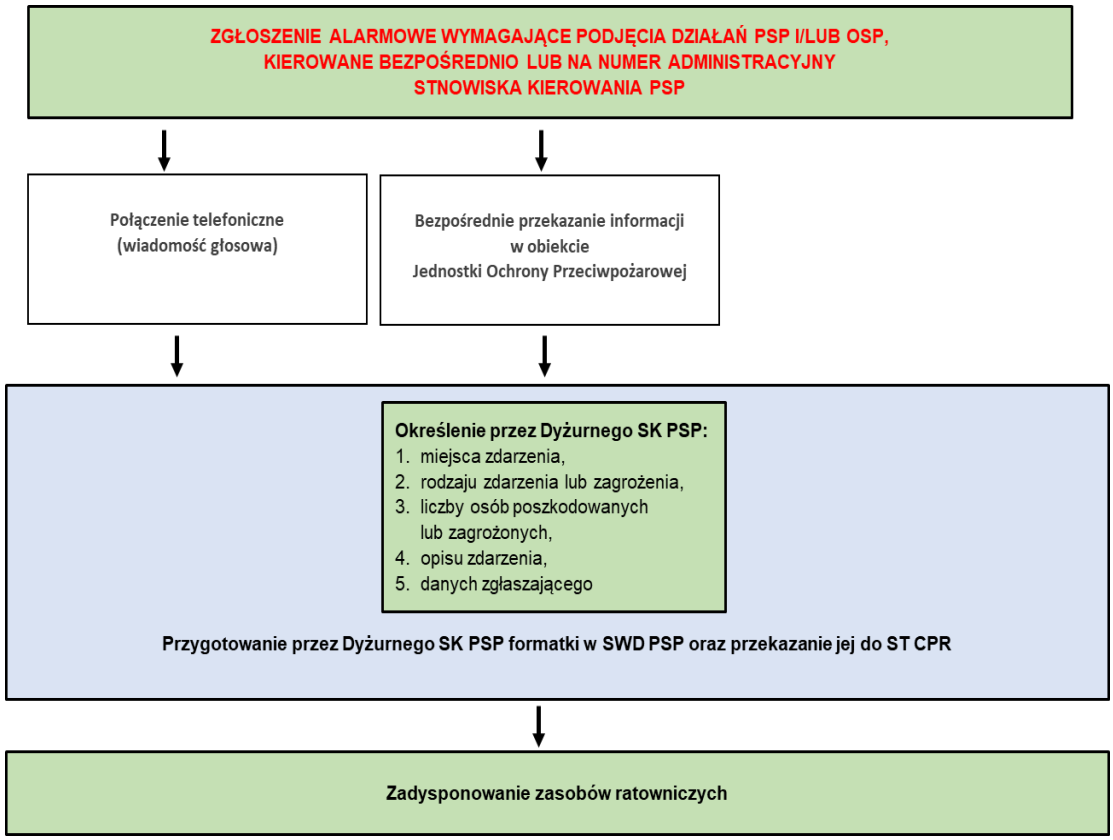
Obsługa zgłoszeń alarmowych innych niż głosowe (SMS, eCall) przychodzących na numery obsługiwane w ramach systemu powiadamiania ratunkowego odbywa się według następującej ogólnej procedury:

- odbiór zgłoszenia alarmowego;
- zarejestrowanie zgłoszenia alarmowego w systemie teleinformatycznym;
- przekazanie zgłoszenia alarmowego właściwemu dyspozytorowi lub dyspozytorom zawierającego w szczególności:
- unikatowy identyfikator zgłoszenia alarmowego,
- informację o dacie i godzinie przyjęcia zgłoszenia alarmowego,
- informację o miejscu zdarzenia lub zagrożenia, umożliwiającą szybkie dotarcie właściwych podmiotów ratowniczych,
- opis zdarzenia lub zagrożenia,
- identyfikator operatora numerów alarmowych, który przyjął zgłoszenie alarmowe,

- informacje o podmiocie lub podmiotach ratowniczych, do których skierowano zgłoszenie alarmowe,
- rodzaj zdarzenia lub zagrożenia według katalogu zdarzeń, o którym mowa powyżej,
- informacje dotyczące lokalizacji zakończenia sieci, z którego zostało wykonane zgłoszenie alarmowe;
- odbiór potwierdzenia przyjęcia zgłoszenia alarmowego przez właściwego dyspozytora.

Poniżej przedstawiono szczegółową procedurę sposobu obsługi zgłoszenia alarmowego wymagającego podjęcia działań przez PSP i/lub OSP kierowanego do numeru alarmowego w CPR:

Natomiast na poniższym schemacie przedstawiono szczegółową procedurę sposobu obsługi zgłoszenia alarmowego wymagającego podjęcia działań przez PSP i/lub OSP kierowanego bezpośredni do SK PSP lub na numer administracyjny SK PSP.



Źródło: Opracowanie własne.

Rysunek 3-3
Przebieg zgłoszenia alarmowego przekazywanego bezpośrednio do stanowiska kierowania PSP.

3.3 ZAGROŻENIA SYSTEMU INFORMACYJNEGO PAŃSTWOWEJ STRAŻY POŻARNEJ.

Podczas omawiania tematyki zagadnień związanych z zagrożeniami bezpieczeństwa informacji w Państwowe Straży Pożarnej warto zwrócić uwagę na posługiwanie się modelami wskazującymi precyzyjny opis poszczególnych elementów i scenariuszy, w których należy uwzględnić podstawowe ogniwa jakimi są poufność, integralność i dostępność.

Mając na względzie zapobieganie różnego rodzaju atakom, należy również oszacować rodzaje strat i uszczerbku, które mogą wystąpić w rezultacie takich ataków w opisywanej organizacji odpowiedzialnej za zapewnienie bezpieczeństwa wewnętrznego państwa. Działania przestępcze ze strony agresorów (napastników) mogą wpływać na środowisko zarówno wewnętrzne, jak i zewnętrzne instytucji, poprzez przechwytywanie, zakłócanie, modyfikowanie lub podrabianie informacji.

Zagrożenia bezpieczeństwa informacyjnego można zdefiniować również jako „walkę informacyjną", czyli działania ukierunkowane na ochronę, wykorzystanie, uszkodzenie, zniszczenie informacji lub zasobów informacyjnych albo też zaprzeczenie informacjom po to, aby osiągnąć korzyści, jakiś cel lub zwycięstwo nad przeciwnikiem[26].

Podczas omawiania konkretnych zagrożeń, należy określić czym jest ryzyko związane z ich wystąpieniem. Należy je odnosić do prawdopodobieństwa, że podmiot gospodarczy poniesie straty w następstwie podjęcia konkretnego ataku. Ryzyko to takie działanie czy przedsięwzięcie, w którym podmiot oceniający nie jest w stanie oszacować wszystkich rzeczywistych zmiennych lub zmienne te nie dadzą się oszacować na bazie rachunku prawdopodobieństwa. W ujęciu potocznym za ryzyko przyjmuje się pewną miarę lub ocenę zagrożenia wystąpienia jakiegoś niepożądanego zjawiska na skutek podjęcia jakiejś decyzji lub z prawdopodobnych zdarzeń od nas niezależnych. Ryzyko różni się od niepewności tym, że dotyczy zjawisk w pewnej mierze cyklicznych, powtarzalnych, dających się w pewnej mierze skalkulować[27].

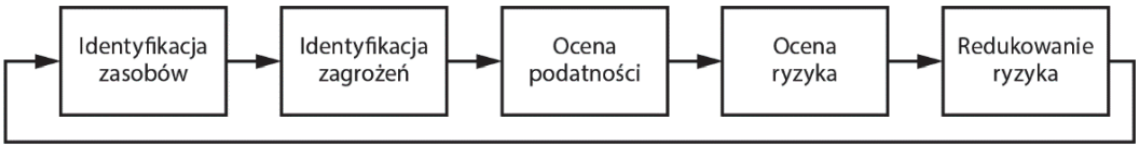
W przypadku przedsiębiorstw i instytucji ryzyko należy rozumieć jako czynnik związany z atakami, które pojawiają się wtedy, gdy występuj jakieś realne zagrożenie, przy czym

[26] Schwartau, Information Warfare, New York 1994. Por.: P. Bączek*, Zagrożenia informacyjne a bezpieczeństwo państwa polskiego*, Wydawnictwo Adam Marszałek, Toruń 2005, s. 132.
[27] W. Šmid, *Boss leksykon*, Wydawnictwo Dr Lex, Kraków, 2012 r., s. 476.

równocześnie istnieją podatności i luki w zabezpieczeniach systemowych danej organizacji, a które napastnik może wykorzystać[28].

Podając za E.Szczepanik „Ryzyko w działalności gospodarczej" można wyróżnić kilka podstawowych obszarów ryzykogennych występujących w działalności instytucji, czy przedsiębiorstwa i należą do nich:

- Działalność inwestycyjna – jest zagrożona poniesieniem wyższych niż planowano kosztów inwestycyjnych, nieplanowanym wydłużeniem cyklu inwestycyjnego, wydłużeniem terminu budowy nowego obiektu, wyższymi kosztami eksploatacyjnymi zakończonej inwestycji.
- Rynkowa działalność przedsiębiorstwa – zaliczyć należy tutaj niespodziewane zmiany w popycie na produkty firmy, ujemny wpływ możliwości sprzedaży wyrobów ze względu na konkurencie (oferta odbiorcom wyrobów lepszych i tańszych).
- Realizacja innowacji technicznych – zagrożeniem jest sytuacja, kiedy nowe konstrukcje mogą okazać się bardzo kosztowne (a przy tym np. mało przydatne) lub okazały się nieudane i nieposiadające zakładanego zastosowania (nietrafione).
- Gospodarka finansowa – pułapkami zawierającymi zagrożenia może być niewypłacalność dłużników, zmiany kursów walut.[29]



Źródło: J. Andress, *Podstawy Bezpieczeństwa informacji – praktyczne wprowadzenie*, Helion S.A. 2019, str. 25

Rysunek 3-4
Etapy procesu zarządzania ryzykiem.

Aby wyeliminować omawiane ryzyko, należy zastosować trzy główne rodzaje mechanizmów obronnych:

- fizyczne,
- logiczne
- administracyjne.

[28] J. Andress, *Podstawy Bezpieczeństwa informacji – praktyczne wprowadzenie,* Helion S.A. 2019, str. 39.
[29] E. Szczepanik, *Ryzyko w działalności gospodarczej*, Wydawnictwo Wyższej Szkoły Menedżerskiej w Warszawie, Warszawa 2010 r., s. 17.

Jest to szczególnie ważne w świecie bezpieczeństwa informacji, co ma na celu wyeliminowanie bądź skuteczne opóźnienie działań napastnika. Należy rozważyć koncepcję obrony w głąb, zwanej również wielopoziomową. W celu skutecznej ochrony środowiska informacyjnego Państwowej Straży Pożarnej należy wprowadzić wiele warstw obrony, ukierunkowanych na możliwość wykrywania ataków i umożliwienie bardziej aktywnej obrony. Tylko przez takie podejście menadżerów, decydentów instytucji, firm i organizacji można uzyskać duże możliwości podniesienia znaczenia działań dla bezpieczeństwa informacji.

System bezpieczeństwa informacyjnego powinien składać się z trzech ściśle powiązanych ze sobą i wchodzących w różne korelacje podsystemów.

Pierwszym z nich jest systemu bezpieczeństwa fizycznego. W ramach takiego systemu zasoby informacyjne powinny zostać fizycznie oddzielone od otoczenia, poprzez stosowanie kontroli dostępu: np. fizyczne zabezpieczenia pomieszczeń, w których znajdują się serwery.

Dotyczy to także informacji niechronionych na podstawie regulacji ustawowych (tzw. danych jawnych). Wówczas ochrona fizyczna koncentruje się między innymi na niedopuszczaniu do zniszczenia fizycznego nośników informacji, tak aby zapobiec ich utraceniu.

Kolejny to system bezpieczeństwa personalnego. Polega on na określeniu kręgu podmiotów i użytkowników, które mają przypisany różny stopień uprawnień dostępu. Można zatem wyróżnić osoby, które mają fizycznie dostęp do nośników informacji lub mają tylko dostęp do zasobów informacyjnych w całości lub w części. Na tym poziomie zabezpieczeń można nadawać różnego rodzaju uprawnienia do wprowadzania zmian w systemie np. dodawania nowych rekordów, usuwania rekordów czy ich edytowania w formie zmiany treści.

Jako trzeci podsystem bezpieczeństwa informacyjnego należy uznać dostęp do elektronicznego przetwarzania informacji. W skład takiego systemu wchodzą narzędzia pozwalające na zachowanie kontroli dostępu, dystrybucji uprawnień, zapobieganie nieuprawnionemu dostępowi, zapobieganie nieuprawnionej instalacji złośliwego oprogramowania itp.[30]

Ataki mogą być przeprowadzane na wiele sposobów i na wielu różnych płaszczyznach. Można je podzielić ze względu na rodzaj ataku, ryzyko, jakie ze sobą niesie oraz mechanizmy zabezpieczające, które wdraża się w celu ich ograniczenia.

[30] P. Liedel, P. Piasecka, T. R. Aleksandrowicz, *Analiza informacji. Teoria i praktyka zarządzanie bezpieczeństwem*, Difin, Warszawa 2012, s. 29-30.

Ataki można ogólnie podzielić na cztery kategorie:

- przechwycenie (ang. interception),
- przerywanie (ang. interruption),
- modyfikowanie (ang. modification)
- podrabianie (ang. fabrication).

.

Źródło: J. Andress, *Podstawy Bezpieczeństwa informacji – praktyczne wprowadzenie*, Helion S.A. 2019, str. 25

Rysunek 3-5
Kategorie ataków - Triada CIA

Ataki przechwytujące umożliwiają napastnikom (osobom bez autoryzacji) dostęp do danych, aplikacji lub środowiska i są przede wszystkim atakami przeciwko poufności. Przechwytywanie może przybrać formę:

- nieautoryzowanego przeglądania lub kopiowania plików,
- podsłuchiwania rozmów telefonicznych lub czytania cudzych wiadomości e-mail,
- można je przeprowadzić na dane, które nie są w trakcie przenoszenia z jednego miejsca na drugie (znajdują się na przykład na dysku twardym, czy w pamięci flash lub są przechowywane w bazie danych.),
- można je przeprowadzić na dane, które przemieszczają się z jednego miejsca do drugiego (korzystanie z bankowości internetowej, wrażliwe, poufne dane przesyłane).

Prawidłowo przeprowadzone ataki przechwytujące co do zasady są bardzo trudne do wykrycia.

Ataki przerywające, zwane także jako zakłócające działanie danego systemu sprawiają, że zasoby instytucji mogą stać się tymczasowo lub na stałe bezużyteczne, bądź niedostępne. Ataki takie zazwyczaj wpływają na dostępność, ale mogą również wpływać na integralność.

Ataki modyfikujące polegają na manipulowaniu zasobami informacyjnymi danej instytucji. Takie ataki mogą być przede wszystkim uważane za ataki dotyczące integralności, ale mogą również zostać sklasyfikowane jako ataki na dostępność.

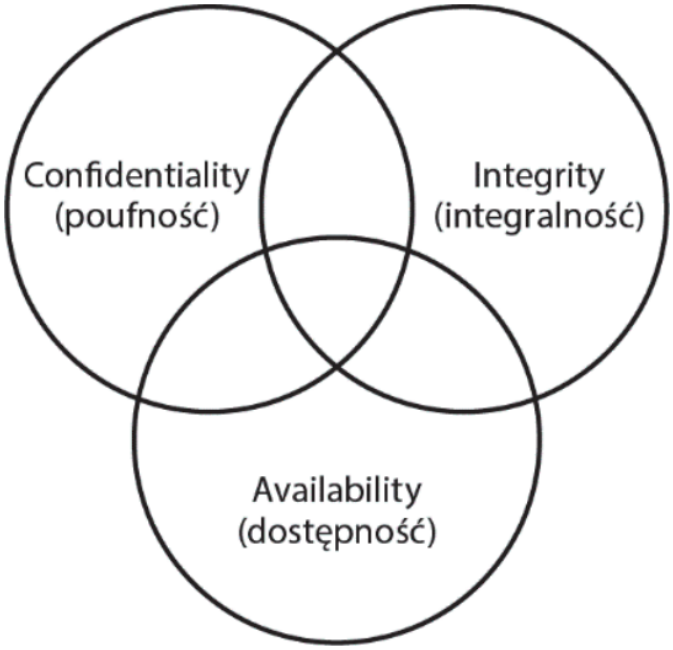
Ataki z podrabianiem polegają na generowaniu danych, procesów, komunikacji lub innych podobnych elementów systemu. Wpływają przede wszystkim na integralność, ale mogą również wpływać na dostępność.

Bezpieczeństwo informacji jest przedmiotem podstawowej, codziennej dbałości kadry kierowniczej Państwowej Straży Pożarnej, ze względu na przetwarzanie różnego rodzaju danych osobowych, finansowych, medycznych itp. Tym bardziej należy przykładać do tego dużą wagę w instytucjach odpowiedzialnych za bezpieczeństwo narodowe naszego kraju.

Skłania to do wniosku i podjęcia decyzji, iż inwestycja w bezpieczeństwo informacji, jest podstawową wartością omawianej organizacji, gdyż konsekwencje naruszeń w tym zakresie są bardzo poważne i kosztowne.

Utrata kontroli nad danymi krytycznymi lub wrażliwymi należącymi do organizacji, prowadzi do utraty wiarygodności, i obniżenia ocen działalności danej instytucji. Naraża to przedsiębiorstwo także na kary, czy też pozwy sądowe. W ostateczności może to doprowadzić do zwolnienia osób odpowiedzialnych za zapewnienie bezpieczeństwa informacji w danej organizacji. Aby tego uniknąć należy wdrożyć odpowiednie formy przeciwdziałania.

Jak już wspomniano na wstępie niniejszego podrozdziału trzema podstawowymi atrybutami zapewniającymi bezpieczeństwo informacji jest poufności, integralności i dostępności, powszechnie określanych w literaturze jako triada PID lub triada CIA (od ang. Confidentiality, Integrity and Availability).



Źródło: J. Andress*, Podstawy Bezpieczeństwa informacji – praktyczne wprowadzenie*, Helion S.A. 2019, str. 21

Rysunek 3-6
Triada CIA

Pojęcie bezpieczeństwa informacji wiąże się z uwzględnieniem poufności, dostępności i integralności informacji. Natomiast bezpieczeństwo danych należy wiązać wzięciem tych trzech elementów pod ochronę, czyli zadbanie o ich bezpieczeństwo, jeśli chodzi o nieodpowiednie lub niekompetentne, celowe bądź omyłkowe wyjawienie, przekształcenie czy też zepsucie.

Poufność odnosić należy do zdolności ochrony danych przed osobami, które nie są upoważnione do ich przeglądania. Poufność informacji oznacza, że dostęp do niej jest ograniczony do wybranej grupy osób lub jednostki, które mają odpowiednie uprawnienia do jej przetwarzania. Celem zapewnienia poufności jest ochrona danych przed dostępem przez osoby do tego nieupoważnione, co pozwala na zachowanie integralności, wiarygodności i poufności informacji.

Znaczenie poufności informacji jest bardzo ważne dla Państwowej Straży Pożarnej. Pozwala to na ochronę strategicznych danych i tajemnic państwowych czy handlowych przed niepożądanym przedostaniem się do podmiotów nieuprawnionych lub przed działaniami osób trzecich. Poufność informacji jest również niezmiernie ważna dla zachowania reputacji, oceny i zaufania społeczeństwa, partnerów i interesariuszy.

Poufność może zostać naruszona na wiele sposobów:

- zgubienie sprzętu zawierającego wrażliwe lub chronione dane,
- wykradzenie hasła przez osoby niepożądane,
- omyłkowe, nieświadome dołączenie do e-maila załączników z poufnymi informacjami do niewłaściwej osoby
- świadome, celowe przeniknięcie napastnika do systemu i uzyskanie dostępu do wrażliwych informacji.

Chronienie poufności informacji jest również ważne ze względów prawnych. Państwowa Straż Pożarna prawny obowiązek ochrony danych osobowych swoich pracowników i interesariuszy, w tym danych wrażliwych i niejawnych. Jeśli organizacja nie chroni poufnie informacji, naraża się odpowiedzialność prawną i duże kary finansowe.

Integralność to natomiast zdolność do zapobiegania zmianom danych w nieuprawniony lub niepożądany sposób. Aby zachować integralność, należy zapewnić w procesach instytucji środki zapobiegające nieautoryzowanym zmianom danych, ale także możliwość cofnięcia niechcianych, autoryzowanych zmian.

Innymi słowy przez pojęcie integralności danych należy rozumieć sytuację, w której dane nie pozostaną w jakikolwiek niekompetentny sposób przekształcone, a co za tym idzie, ich stan będzie kompatybilny z wymaganym i spodziewanym stanem faktycznym[31].

Integralność jest szczególnie ważna, gdy dotyczy danych, które stanowią podstawę podejmowania ważnych decyzji, co jest codziennością w procesach Państwowej Straży Pożarnej.

Zadaniem integralności jest zadbanie o to, aby dane były skrupulatne, wyczerpujące oraz istotne a także o dopilnowanie, by informacje nie uległy przypadkowemu czy też świadomemu przeinaczeniu informacji[32].

Przyczynami, które mogą zakłócić integralność danych w organizacji to m.in.[33]:

- czynności podejmowane przez niekompetentnego, bądź niestarannego pracownika/użytkownika systemu bądź procesu,
- działania wirusów, złośliwego oprogramowania,

[31] E. Dudek, M Kozłowski., *Zagadnienie bezpieczeństwa zintegrowanych informacji operacyjnych w porcie lotniczym Logistyka 4*, Warszawa 2010 r., s.183-192.

[32] A. Czarnecki, *Bezpieczeństwo systemów informatycznych*. Case studies w informatyce, Wyższa Szkoła Bankowa w Gdańsku, 2015 r., s.412-420.

[33] E. Golis, Banasiak J., *Badania realizacji zasad bezpieczeństwa danych w systemach komputerowych małych firm*, Prace Naukowe akademii im. Jana Długosza w Częstochowie, Edukacja Techniczna i Informatyczna, Nr 6, 2011 r., s.101-107.

- uszkodzenia, niesprawności,
- nieprawidłowości w posiadanym oprogramowaniu,
- awaria w transmisji.

Zapewnienie integralności danych powinno zostać zagwarantowane podczas przekazywania, przekształcania i przetrzymywania informacji. Na podstawie analizy literatury można wyróżnić sprawdzone sposoby, które bez wątpienia wpływają na zagwarantowanie integralności danych:

- ujawnienie każdej ewentualności bądź próby zakłócenia integralności danych,
- ograniczenie, obniżenie ilości autoryzacji dostępu,
- przygotowanie i wdrożenie procedur, mających na celu uwierzytelnienie,
- redukowanie faktycznego wglądu do systemów będących w zasobach organizacji,
- stosowanie nowoczesnych systemów operacyjnych z możliwością zaimplementowania odpowiednich mechanizmów uprawnień ograniczających działania, jakie nieautoryzowany użytkownik może wykonać na danym pliku np. właściciel pliku może mieć uprawnienia do odczytu i zapisu, podczas gdy inni użytkownicy mogą mieć uprawnienia tylko do odczytu pliku lub w ogóle mogą nie mieć do niego dostępu.

Strategia, która ma na celu zagwarantowanie integralności danych, to w rzeczywistości zespół zasad, procedur i zarządzeń, które odnoszą się do metod zapewnienia przez systemy stanu, iż przechowywane i ukazywane dane pokrywają się i odpowiadają postawionym wymaganiom. Każda taka strategia powinna zapewniać wymóg, aby dane w systemach były nienaganne i bezbłędne. Dane, które są otrzymywane powinny być sortowane, a następnie, po przefiltrowaniu, zostaną wewnętrznie magazynowane i zabezpieczone. Zachowanie tego kryterium, zapobiega ponownemu przetwarzaniu danych bazowych - otrzymanych na początku procesu[34].

Kolejnym atrybutem triady CIA jest dostępność informacji, która polega na zapewnieniu swobodnej, łatwej osiągalności informacji przez użytkowników systemów. Pozwala to odbiorcy na szybkie i wygodne skorzystanie z danych dostępnych w bazach danych lub w innych źródłach. Pozwala ona na przetwarzanie informacji w sposób efektywny i wydajny, co przekłada się na wzrost produktywności i oszczędności.

Dla zapewnienia odpowiedniego poziomu dostępności, niezbędne jest:

- ustanowienie i wdrożenie polityki dostępności informacji,

[34] C. Henderson, *Skalowalne witryny internetowe. Budowa, skalowanie i optymalizacja aplikacji internetowych nowej generacji*, Helion S.A., 2007 r., s. 222.

- wdrożenie wydajnego i bezpiecznego systemu przechowywania informacji, który ponadto jest łatwy w użyciu,
- zapewnienie systemu do tworzenia i edycji informacji, który gwarantuje zgodność z wymaganiami,
- wdrożenie procedur, które zapewnią, że informacje są aktualizowane.

Dostępność można utracić np. z powodu:

- awarii zasilania,
- problemów z systemem operacyjnym lub z aplikacjami,
- ataków sieciowych czy naruszenia bezpieczeństwa systemu.

Niezależnie od wdrożonych systemów bezpieczeństwa informacji za najsłabsze ogniowo systemu zabezpieczeń należy uznać „ogniwo ludzkie". Omawiane w literaturze, ale wynikające także z doświadczenia zawodowego autora niniejszej dysertacji przykłady zachowań pracowniczych naruszające zasady bezpieczeństwa to:

- klikanie niebezpiecznych linków,
- wysyłanie poufnych informacji niezabezpieczonymi kanałami,
- przekazywanie haseł
- umieszczanie ważnych danych w widocznych miejscach.
- wykorzystywanie niefrasobliwych zachowania użytkowników do przeprowadzania ataków socjotechnicznych - manipulacja ludźmi w celu zdobycia informacji lub dostępu do chronionych obiektów.

Należy podjąć działania mające na celu ochronę instytucji przed takimi zagrożeniami, ustalając odpowiednie procedury i zasady. Niezbędnym aspektem jest także ustawiczne szkolenie pracowników rozpoznawania tego typu zagrożeń.

Człowiek w dzisiejszym świecie jest przeinformowany, otoczony gąszczem zbędnych informacji, które naruszają jego indywidualizm i godzą w wolna wolę[35].

Natomiast do problemów informacyjnych współczesności zaliczyć należy[36].

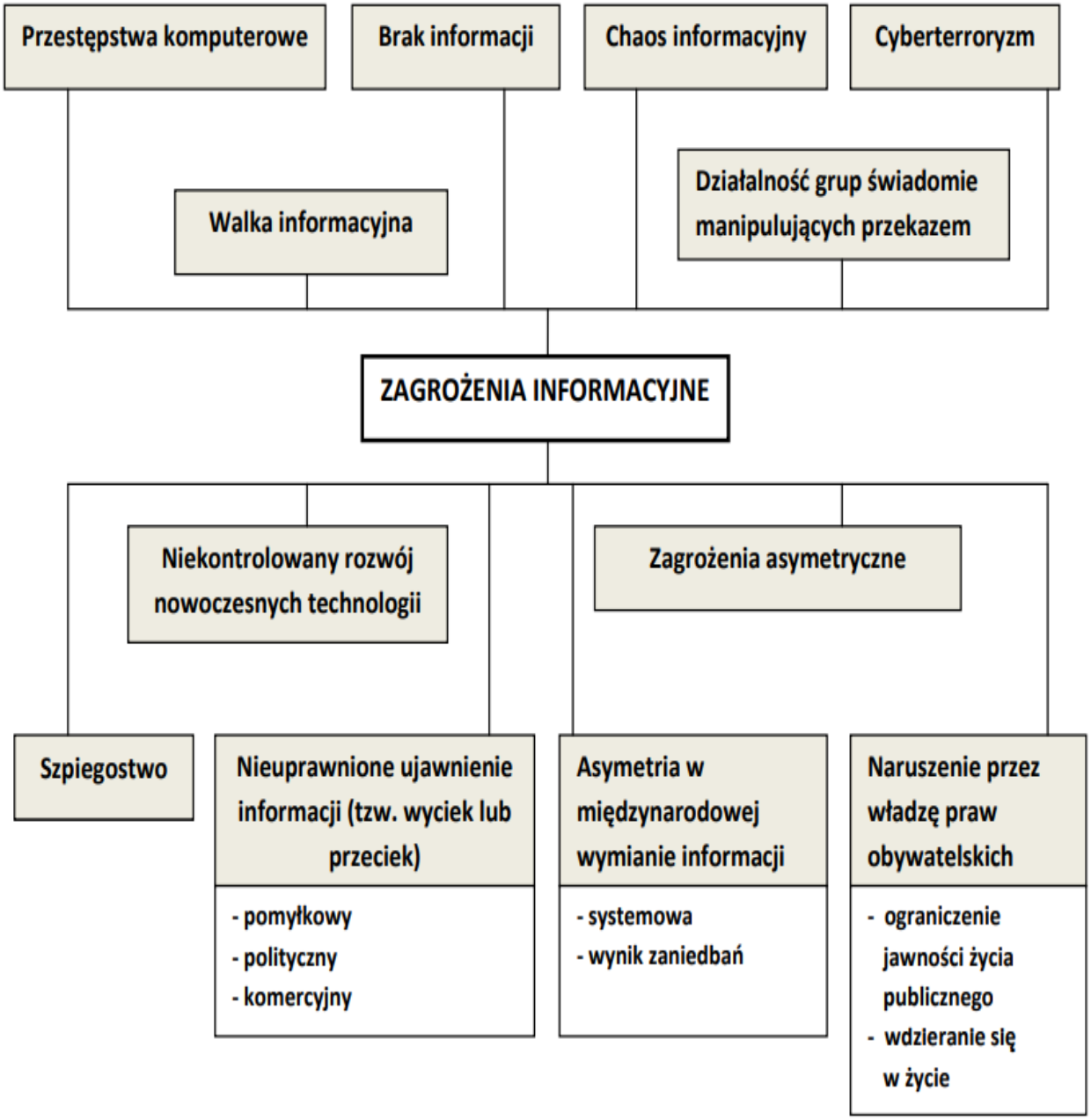
- nadmiar informacji;
- szum informacyjny;
- stres informacyjny;

---

[35] N. Postman, Technopol. *Triumf techniki nad kulturą*, Warszawa 1995, s. 246 [w:] W. Babik, *O niektórych zjawiskach towarzyszących odbiorowi informacji: percepcja informacji w świetle ekologii informacji*, Kraków
2008, s. 5.

[36] K. Materska, *Ekologiczne zarządzanie informacją, Przegląd informacyjno-dokumentacyjny*, 2005, nr 2 (289), s. 29-44.

- niskie kompetencje informacyjne odbiorców informacji;
- dylematy etyczne;
- rozbieżność informacyjną.



Źródło: P. Bączek, *Zagrożenia informacyjne a bezpieczeństwo państwa polskiego*, Wydawnictwo Adam Marszałek, Toruń 2006, s. 30

Rysunek 3-7
Podział zagrożeń informacyjnych

Reasumując powyższe rozważania, opierając się na wnikliwej analizie literatury, ale także doświadczeniach własnych autora dysertacji, można przyjąć założenie, że największymi zagrożeniami w stosunku do bezpieczeństwa systemu informacyjnego Państwowej Straży Pożarnej są:

- czynnik ludzki (zarówno sami pracownicy organizacji, jak i „napastnicy" zewnętrzni"):
  - terroryzm,
  - cyberprzestępczość - ataki hackerskie,
  - celowe działania pracowników - uszkadzanie sprzętu lub danych;
  - udostępnianie zasobów informacyjnych osobom nieuprawnionym np. mediom,
  - przypadkowe lub świadome wykasowanie plików (utrata informacji);
  - błędy w montażu podzespołów sieci lub urządzeń prowadzące do ich awarii;
  - tworzenie tzw. szumu informacyjnego w przekazie informacji
  - brak szkoleń pracowników;
  - brak odpowiedniego poziomu kontroli i nadzoru ze strony kadry dowódczej;
- siły natury – katastrofy naturalne, przybierające np. postaci:
  - zalań urządzeń bądź pomieszczeń serwerowni;
  - pożarów pomieszczeń lub całych budynków (zasobów materiałowych PSP), co w konsekwencji prowadzi do utraty danych,
  - wiatrów uszkadzających sieci przesyłowe, w tym energetyczne;
- wady techniczne sprzętu, awarie wywołane słabą jakością sprzętu – kupowanie na zasadach przetargów publicznych z kryterium najniższej ceny,
- brak właściwych rozwiązań organizacyjno-prawnych (brak całościowej polityki bezpieczeństwa informacji),
- niewłaściwa struktura organizacyjna jednostki.

3.4 POLITYKA BEZPIECZEŃSTWA INFORMACJI W PAŃSTWOWEJ STRAŻY POŻARNEJ.

Najogólniej rzecz ujmując polityka bezpieczeństwa informacji to zestaw uwierzytelnionych procedur i zasad bezpieczeństwa razem z programem na ich wprowadzenie oraz egzekwowanie.[37] Bezpieczeństwo informacji rozumiane jest tu jako moment, w którym nie ma zagrożenia,[38] co wiąże się z nieprzerwanym działaniem procesów instytucji. Jest to stan, w którym informacje należące do instytucji nie są zagrożone[39].

Do aspektów bezpieczeństwa informacji zaliczyć należy:

- dostępność,
- poufność,
- niezawodność,
- integralność,
- autentyczność[40].

Dostępność należy rozumieć jako udostępnianie informacji osobą do tego upoważnionym, natomiast poufność jako nieudostępnianie nieodpowiednim osobą. Integralność to zapewnienie kompletności i dokładności, a autentyczność oznaczać będzie prawdziwość informacji. Niezawodność oznacza zaś spełnianie określonych zadań w odpowiednim czasie.

Do celów w zakresie gwarancji bezpieczeństwa i ochrony informacji należą[41].

- zagwarantowanie bezpiecznego oraz poprawnego funkcjonowania systemów, które zajmują się przetwarzaniem informacji,
- całkowite zmniejszenie możliwości pojawienia się niebezpieczeństw w stosunku do informacji,
- gwarancja odpowiedniego poziomu bezpieczeństwa informacji, które są przetwarzane.

Polityka bezpieczeństwa informacji to zestaw dokumentów, które regulują zasady, jak i metody i techniki zapewniania bezpieczeństwa i ochrony informacji. Polityka bezpieczeństwa jest odniesieniem do formowania dokumentów, które są wzorcami warunków, jakie muszą pozostać spełnione przez systemy funkcjonujące w danej organizacji, zarówno

[37] Rozporządzenie Rady Ministrów w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (2012) Dz. U. 2012 poz. 526. art. 2.
[38] A. Białas, *Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie,* WNT, Warszawa, 2007 r. s. 27.
[39] J. Łuczak, *Ochrona danych osobowych jako element zarządzania bezpieczeństwem informacji*, 2016 r. s. 59.
[40] A. Białas, *Bezpieczeństwo…,*op.cit.,37.
[41] M. Kowalewski*, Polityka…*, op.cit., 4.

te papierowe, jak i informatyczne. Powinna ona określać także wymagania dla poszczególnych grup informacji. Uwzględnia się tutaj aspekt prawny systemów informatycznych oraz ochrony informacji[42].

Obejmuje ona swoim zakresem takie elementy, jak: politykę informacyjną, ochronę informacji niejawnych, zasady ochrony danych osobowych, politykę bezpieczeństwa systemu teleinformatycznego, zasady ochrony tajemnicy przedsiębiorstwa lub innych tajemnic zawodowych, zapobieganie przestępstwom na szkodę instytucji, szczególnie fałszerstwom i oszustwom, zasady ochrony fizycznej i technicznej, i inne związane z bezpieczeństwem[43].

Istotnym jest, aby polityka bezpieczeństwa informacji była zgodna z aktualnie obowiązującym prawem. Należy ją opracować na podstawie obecnie obowiązujących rozporządzeń oraz ustaw dotyczących między innymi ochrony praw autorskich i danych osobowych czy ochrony informacji niejawnych.

Podczas opracowywania odpowiedniej polityki bezpieczeństwa informacji należy uwzględnić wiele czynników związanych z daną organizacją, do których należą między innymi:

- specyfika funkcjonowania organizacji,
- wszelkiego rodzaju procesy zachodzące w tej instytucji,
- charakter organizacji,
- struktura organizacji.

Politykę bezpieczeństwa informacji powinna obejmować wszystkich pracowników określonej instytucji. Powinna ona być stale aktualizowana.

Informacje na temat wdrożenia i opracowania polityki bezpieczeństwa można odnaleźć w opracowanym przez GIODO dokumencie pt. "Wytyczne w zakresie opracowania i wdrożenia polityki bezpieczeństwa". Polityka bezpieczeństwa dotyczy całościowego problemu zabezpieczenia danych. Odnosi się do danych które są przetwarzane tradycyjnie jak również do danych przetwarzanych w systemach informatycznych. Dlatego każdy podmiot przetwarzający dane osobowe jest zobowiązany przygotować i stosować się do polityki bezpieczeństwa, nawet jeśli nie korzysta z komputerów do tego celu[44].

Głównymi celami opracowania i wdrożenia polityki bezpieczeństwa są stworzenie reguł i zasad postępowania oraz wskazanie algorytmów działań jakie należy podjąć, aby

[42] M. Kowalewski, A. Ołtarzewska, *Polityka*…, op.cit., s. 4.
[43] Encyklopedia zarządzania – wersja online, hasło *Zasady ochrony tajemnicy przedsiębiorstw* (dostęp 2022-10-23)
[44] L. Kępa, *Ochrona Danych Osobowych w Praktyce*, Warszawa 2014 s. 272-274.

poprawnie zabezpieczyć dane. W ramach właściwego funkcjonowania polityki bezpieczeństwa nie powinno umieszczać się w niej zapisów podlegających częstym zmianom, a także zawierających w treściach informacji szczegółowej. W przeciwnym wypadku prowadziłoby to do częstego przyjmowania nowych dokumentów.

Polityka ta musi być opracowana w formie pisemnej, i przedstawiona każdemu zatrudnionemu pracownikowi, który ma dostęp do przetwarzania danych osobowych, z obowiązkiem pisemnego potwierdzenia o zapoznaniu się z jej treścią. Pracownicy powinni być zapoznani z tymi regulacjami na samym początku zatrudnienia zanim rozpoczną działania w procesie przetwarzania danych osobowych[45].

Jeśli chodzi o strukturę polityki bezpieczeństwa to powinna zawierać ona[46]:

- wykaz budynków oraz pomieszczeń w których będzie odbywał się proces przetwarzania danych osobowych
- wykaz zbiorów danych a także wskazanie programów które znajdą zastosowanie w procesie przetwarzania danych
- informacje dotyczące przepływu danych pomiędzy systemami
- opis środków organizacyjnych jak i technicznych które są gwarantem poufności, integralności i rozliczalności przetwarzanych danych
- opis struktury zgromadzonych danych który wskazuje na powiązania między poszczególnymi polami informacyjnymi

Oczywiście przedstawiony powyżej zakres informacji stanowi wymogi podstawowe i należy podkreślić, że polityka bezpieczeństwa może, a nawet powinna być wzbogacona o większy zakres informacji.

Polska Norma PN-ISO/IEC 27001 wskazuje, że celem polityki bezpieczeństwa jest wsparcie kierownictwa dla bezpieczeństwa informacji oraz zapewnienie jej kierunków działań. Polityka bezpieczeństwa ma zawierać zbiór zasad i praktyk wraz z dokumentacją w jaki sposób organizacja ma chronić przetwarzane dane osobowe.

Aby polityka bezpieczeństwa była zgodna z powyższą normą ISO to dodatkowo powinny się w niej znaleźć następujące informacje:

- definicja bezpieczeństwa informacji,
- podkreślenie intencji kierownictwa,
- definicje ogólnych obowiązków w zakresie zarządzania bezpieczeństwem informacji itp.

[45] L. Kępa, *Zasady*…, op.cit., s. 272-274.
[46] Encyklopedia zarządzania – wersja online, hasło *Struktura polityki bezpieczeństwa* (dostęp 2023-01-23).

Polityka bezpieczeństwa traktowana jest jako dokument wewnętrzny instytucji i nie musi stanowić dokumentu publicznie dostępnego[47].

Podając za K. Liderman osiągnięcie sukcesu przy wdrażaniu polityki bezpieczeństwa powinno być oparte m.in. na podniesieniu świadomości i chęci kadry kierowniczej w celu podniesienia bezpieczeństwa informacyjnego, przy zapewnieniu i przeznaczeniu odpowiednich środków finansowych na ten cel. Powinno to wiązać się również z podjęciem decyzji co do sposobu budowy bądź modyfikacji systemu bezpieczeństwa informacyjnego[48].

W Państwowej Straży Pożarnej duży nacisk kładzie się na politykę ochrony danych osobowych.

W normach prawnych poszczególnych krajów rozwiniętych ochrona danych osobowych nie ma sprecyzowanej stałej, jednolitej definicji. Można przyjąć natomiast, że dane osobowe to każda informacja dotycząca konkretnej osoby, którą można zidentyfikować - wynika z tego fakt braku anonimowości.

W dużym uproszczeniu można przyjąć, że dane osobowe stanowi połączenie imienia i nazwiska z innymi danymi osoby, np. numerem PESEL, NIP, datą urodzenia, ocenami studenta itp.

Natomiast za informacje osobowe nie będą uznawane dane o charakterze osobowym, które nie są powiązane z konkretną osobą, której tożsamość na ich podstawie można by ustalić, a ujawnienie ich nie stanowi żadnego zagrożenia dla prywatności tej osoby[49].

Przetwarzanie danych to wszystkie operacje i czynności dokonywane na danych osobowych, najczęściej w systemach informatycznych. Zaliczyć możemy do nich: zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie, a nawet ich usuwanie. Przyjmuje się w komentarzach i orzecznictwie, że pod poszczególnymi wymienionymi powyżej pojęciami rozumie się ich znaczenie zawarte w słownikach.

Podając za E. Śleszyńską wyróżniamy cztery etapy przetwarzania danych w systemach informatycznych[50].

- etap polegający na zbieraniu danych,
- etap polegający na utrwalan, przechowywaniu, zmienianiu danych,
- etap polegający na udostępnianiu danych,

[47] L. Kępa, *Ochrona…* op.cit., s. 272-274.
[48] K. Liderman, Bezpieczeństwo…, op.cit., s. 229-230.
[49] A. Mednis, *Prawna ochrona danych osobowych*, Wydawnictwo prawnicze, Warszawa 1995 r., s. 14.
[50] E. Śleszyńska, *"Administrowanie danymi osobowymi przez zarządców i właścicieli nieruchomości*", Wydawnictwo Wolters Kluwer, Warszawa 2008 r., s. 5.

- etap polegający na usuwaniu danych.

Jako podstawowe warunki przetwarzania danych można przyjąć natomiast[51]:

- warunki generalne (pomijające fakt o jaką postać przetwarzania danych chodzi), w rozbiciu na:
  1. warunki dotyczące przetwarzania danych zwykłych,
  2. warunki dotyczące przetwarzania danych wrażliwych.
- warunki odnoszące się do zbierania danych, z podziałem na:
  1. zbieranie od osoby, której dane dotyczą,
  2. zbieranie nie od osoby, której dane dotyczą,
- warunki odnoszące się do udostępniania danych w celach innych niż włączanie do zbioru, które można kwalifikować jako:
  1. udostępnianie podmiotom, które z mocy prawa są uprawnione do otrzymania danych,
  2. udostępnianie podmiotom, które nie są uprawnione do otrzymania danych z mocy prawa, natomiast w sposób wiarygodny uzasadniają potrzebę ich posiadania.

Dane zwykłe są to najbardziej podstawowe dane osobowe, czyli imię i nazwisko, adres zamieszkania lub zameldowania, PESEL, NIP czy numer telefonu. Nie zostały one ustawowo określa wprost, natomiast to one najdokładniej opisują konkretną osobę i są podawane najczęściej.

Dane wrażliwe są to dane wnikające w sferę bardzo prywatną i należą do nich m.in. informacje o: pochodzeniu rasowym czy etnicznym, poglądach politycznych, wyznaniu i przekonaniach religijnych, przynależności partyjnej/związkowej, stanie zdrowia, kodzie genetycznym, nałogach, wyrokach i mandatach karnych[52].

Oprócz podstawowych danych osobowych, w RODO zostały ściśle określone pojęcia danych wrażliwych osób fizycznych. Takie wprowadzenia bezpośrednio dotyczą elektronicznego przetwarzania danych. Do tych danych należą[53].

1. Adres IP – numer przypisany urządzeniu należącemu konkretnemu użytkownikowi.

[51] J. Barta, *"Ochrona danych osobowych: Komentarz*", Wydawnictwo Wolters Kluwer, Warszawa 2011 r., s. 445.
[52] A. Nerka, *"Granice ochrony danych osobowych w stosunkach pracy",* Wydawnictwo Wolters Kluwer, Warszawa 2009 r., s. 19.
[53] PARP, *Ochrona danych osobowych. Poradnik dla małych i średnich przedsiębiorców*, PARP druk, Warszawa 2017 r., s. 16-21.

2. Identyfikator plików cookie – pliki tekstowe generowane przez urządzenia i aplikacje użytkowników, które są wykorzystywane do śledzenia aktywności na stronach internetowych.
3. Adres poczty elektronicznej – adresy, na podstawie których można zidentyfikować bezpośredniego właściciela.
4. Wizerunek osoby fizycznej – zdjęcia użytkowników.
5. Szczególne kategorie danych – są to dane biometryczne, genetyczne i dotyczące zdrowia.

Przetwarzanie danych osobowych jest dopuszczane, gdy[54].

- osoba, której dane dotyczą wyrazi na to zgodę – nie dotyczy to sytuacji usunięcia dotyczących jej danych,
- jest to niezbędne do zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa,
- jest to konieczne do realizacji umowy, gdy osoba, której dane dotyczą, jest jej stroną
- jest to niezbędne do podjęcia działań przed zawarciem umowy na żądanie osoby, której dane dotyczą,
- jest niezbędne do wykonania określonych prawem zadań realizowanych dla dobra publicznego,
- jest to niezbędne do wypełnienia prawnie usprawiedliwionych celów realizowanych przez administratorów danych albo odbiorców danych, a przetwarzanie nie narusza praw i wolności osoby, której dane dotyczą.

Nadmienić tym miejscu należy, że aby przetwarzanie danych odbywało się zgodnie z literą prawa wystarczy spełnienie co najmniej jednego z wymienionych powyżej warunków.

Przetwarzanie danych powoduje obowiązek ich zabezpieczenia, w tym także w systemach informatycznych. Wiąże się to z wdrożenie i obsługą odpowiednich środków technicznych i organizacyjnych, mających na celu zabezpieczenie danych przed nieuprawnionym i niepożądanym ich przetwarzaniem.

Przetwarzanie danych osobowych rozumiane jest tutaj jako czynności faktyczne, a nie do czynności prawne. Aby uznać, że dany podmiot dokonuje przetwarzania danych osobowych wystarczy, by wykonał on jedną z czynności zaliczonych do definicji przetwarzania.

[54] E. Śleszyńska, *Administrowanie danymi osobowymi przez zarządców i właścicieli nieruchomości*, Wydawnictwo Wolters Kluwer, Warszawa, 2008 r., s. 9.

Do przetwarzania danych osobowych uprawniony jest administrator danych, tylko w zakresie i na warunkach zgodnych z prawem[55].

Jednym z pierwszych i zarazem podstawowych aktów prawnych stających w obronie praw i wolności człowieka jest Europejska Konwencja o Ochronie Praw Człowieka i Podstawowych Wolności (Europejska Konwencja Praw Człowieka) z 1950 roku. Przedstawione są w niej i unormowane relacje państwa do ochrony praw, a także wskazane prawa jakie przysługują jednostce prawnej i środki, które służą dochodzenia tych praw.

Kolejno jednym z najważniejszych aktów prawa międzynarodowego, z dziedziny ochrony danych osobowych jest wydana przez Radę Europy Konwencja nr 108 o ochronie osób fizycznych w związku z automatycznym przetwarzaniem danych osobowych z dnia 28 stycznia 1981 roku.

23 września 1980 roku zostały wydane wytyczne w sprawie Ochrony Prywatności i Przekazywania Danych Osobowych Pomiędzy Krajami. Uważa się je obok wspomnianej wyżej Konwencji nr 108 Rady Europy do najważniejszych dokumentów prawa międzynarodowego ostatniego czasu[56].

W polskim prawodawstwie istotnym było wydanie 29 sierpnia 1997 roku Ustawy o ochronie danych osobowych. Ustawa ta wprowadzała nowe uregulowania nieznane zupełnie dotąd w naszym systemie prawnym. Obecnie obowiązująca w tym zakresie jest ustawa dnia 22 stycznia 2004 r. o zmianie ustawy o ochronie danych osobowych oraz ustawy o wynagrodzeniu osób zajmujących kierownicze stanowiska państwowe.

Art. 1. ustawy o ochronie danych osobowych mówi, że każdy obywatel ma prawo do ochrony danych osobowych, a przetwarzanie ich może odbywać się jedynie w sytuacjach określonych daną ustawą[57].

Zasady ochrony danych wynikają bezpośrednio z ustawy o ochronie danych osobowych RODO, która weszła w życie z 25 Maja 2018. RODO określa ramy ochrony danych osobowych, natomiast określenie bezpośrednich zasad pojawiło się już w rozporządzeniu 2016/679 UE. W rozporządzeniu został wprowadzony jednolity katalog zasad prawa ochrony danych[58].

Zgodnie z Rozporządzeniem Parlamentu Europejskiego, Art. 13: "Aby zapewnić spójny stopień ochrony osób fizycznych w Unii oraz zapobiegać rozbieżnościom hamują-

[55] E. Śleszyńska, *Administrowanie*…, op.cit., s. 5-8.
[56] Encyklopedia zarządzania – wersja online, hasło *Prawo międzynarodowe* (dostęp 2022-05-12).
[57] Analizę przeprowadzono na podstawie Ustawy o Ochronie Danych Osobowych (Dz. U. Nr 33, poz. 285).
[58] M. Błażewski, *Środki prawne ochrony danych osobowych. Wprowadzenie do prawa ochrony danych osobowych*, Drukarnia Beta-druk, Wrocław, 2018 r., s. 51.

cym swobodny przepływ danych osobowych na rynku wewnętrznym, należy przyjąć rozporządzenie, które zagwarantuje podmiotom gospodarczym – w tym mikroprzedsiębiorstwom oraz małym i średnim przedsiębiorstwom – pewność prawa i przejrzystość, a osobom fizycznym we wszystkich państwach członkowskich ten sam poziom prawnie egzekwowalnych praw oraz obowiązków i zadań administratorów i podmiotów przetwarzających, które pozwoli spójnie monitorować przetwarzanie danych osobowych, a także które zapewni równoważne kary we wszystkich państwach członkowskich oraz skuteczną współpracę organów nadzorczych z różnych państw członkowskich[59].

Łącznie powstało jedenaście zasad[60].

1. Legalności – określa sposoby przetwarzania i zabezpieczenia danych;
2. Rzetelności – prawa i wolności osób, których dotyczą dane;
3. Privacy be design – zapewnienie środków zabezpieczenia danych osobowych użytkowników;
4. Privacy by default – środki organizacyjne i techniczne do przetwarzania i przechowywania danych osobowych;
5. Przejrzystości – dostępna forma dla użytkowników, zrozumiały przekaz zasad przechowywania i wykorzystania zbieranych danych;
6. Minimalizacji – przetwarzanie jedynie danych niezbędnych dla działania przedsiębiorstwa;
7. Prawidłowości – sposoby usuwania i termin przechowywania zbieranych danych;
8. Integralności i poufności – zabezpieczenie i udostępnienie danych;
9. Ograniczenia celu – cel gromadzenia danych oraz wykorzystanie danych zgodnie z ustalonym celem;
10. Ograniczenia przechowywania – czas trzymania danych;
11. Rozliczalności – opis wdrożonych systemów do ochrony danych lub wykorzystywanych do tego metod i narzędzi.

Zasady te są wzajemnie ze sobą powiązane. Nadrzędnymi są zasady rzetelności i legalności[61]. Natomiast każde przedsiębiorstwo powinno dążyć do jak naj-

[59] Rozporządzenie Parlamentu Europejskiego I rady (UE) 2016/67, (2016), Dz. Urz. UE nr L119/1.
[60] Guidelines on transparency under Regulation 2016/679., s. 6-13.
[61] P. Drobek, *RODO - Ogólne rozporządzenie o ochronie danych. Komentarz*, WKP, Warszawa 2018 r., s 327.

bardziej rzetelnego sposobu przechowywania danych, które polega na równowadze między interesami instytucji a prywatnością osoby fizycznej[62].

Rozbudowane postanowienia dyrektywy 2002/58/WE dotyczą danych osobowych związanych z korzystaniem z usług komunikacji elektronicznej. Oprócz obowiązku zapewnienia poufności treści przekazu art. 5 dyrektywy 2002/58/WE nakładana państwa członkowskie obowiązek zagwarantowania poufności związanych z przekazem danych dotyczących ruchu (Traffic data), przez które dyrektywa rozumie wszelkie dane przetwarzane w celu przesyłania przekazu w sieciach komunikacji elektronicznej lub ustalenia należności z tego tytułu. Dane dotyczące ruchu, określane również mianem danych transmisyjnych mogą posiadać m.in. dane o wyborze drogi (rolling), położeniu terminalu użytkownika, informacji o sieci, czasie rozpoczęcia i zakończenia połączenia oraz formatu, w jakim przekaz jest dokonywany. Dzięki asocjowaniu tych danych z daną osobą możliwe staje się wyciągnięcie informacji o sposobie i zakresie wykorzystania przez tę osobę z usług. W konsekwencji czego naraża osobę na istotne zagrożenia dla prywatności użytkowników. W tym zakresie przyjęta została ogólna zasada przewidująca obowiązek usunięcia takich danych lub poddania ich anonimizacji, z chwilą gdy nie są już potrzebne do transmisji przekazu. Od tej zasady przewidziano kilka wyjątków dotyczących: przetwarzania danych. W celach rozliczeniowych, świadczenia usług o wartości dodanej przetwarzania danych w celach marketingowych oraz wykrywania oszustw, a także w związku z prowadzeniem postępowań przez uprawnione organy. Wykorzystywanie danych w celach marketingowych jest uzależnione od zgody użytkownika. Dyrektywa 2002/58/WE (art. 5 ust.3) jasno ustanawia także kwestię zapisywania i dostępu do informacji przetrzymywanych w terminalu użytkownika (np. pliki Cookies). Dozwolone jest używanie takich technologii, pod warunkiem, że użytkownik zostanie o tym poinformowany oraz, że będzie miał sposobność wyrażenia sprzeciwu. W 2009 r. została dokonana nowelizacja, zmieniająca dotychczasową regułę. W tym zakresie i dopuszcza takie działania, pod warunkiem że abonent lub użytkownik wyraził na to zgodę. Odstępstwo od tej reguły przewidziano jedynie dla technicznego przechowywania danych bądź dostępu do nich jedynie w celu wykonania transmisji komunikatu za pośrednictwem sieci łączności elektronicznej lub gdy jest to niezbędne doświadczenia usługi wyraźnie zażądanej przez abonenta lub użytkownika[63].

[62] M. Krzysztofek, *Komentarz do rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679*, "*Ochrona danych osobowych w Unii Europejskiej po reformie*", CHB, Warszawa 2016 r., s.55-57.
[63] J. Barta, R. Markiewicz, *Ochrona danych osobowych*, Zakamycze, Kraków, 2011 r., s. 254-255.

Polityka prywatności to umowa prawna informująca o zakresie danych osobowych, które są gromadzone podczas przeglądania serwisu internetowego przez odwiedzających go użytkowników. Opisuje ona cele zbierania danych osobowych oraz sposoby ich wykorzystania i zabezpieczenia.

Sposób ochrony danych osobowych jest indywidualnie dostosowany do zakresu realizowanych zadań przedsiębiorstwa. Polityka prywatności występuje dokumentem wewnętrznym przedstawiającym metody zbierania i przetwarzania danych personalnych. Pojęcie przetwarzania danych obejmuje[64]:

- porządkowanie;
- modyfikowanie;
- pobieranie;
- ujawnianie i rozpowszechnianie;
- udostępnianie osobom trzecim;
- łączenie i organizowanie;
- usuwanie, przechowywanie i niszczenie.

Każde przedsiębiorstwo ma obowiązek wyszczególnienia w polityce prywatności sposobu przetwarzania danych po ich stronie oraz przedstawienie systemów zabezpieczania tych informacji[65].

Na podstawie wymienionych wcześniej zasad można przedstawić konspekt na opracowanie polityki prywatności[66].

- Opis podmiotu
- Jakie dane zbieramy? – określenie rodzajów i kategorii przetwarzanych danych osobowych i podstawy prawne które uzasadniają potrzebę przechowywania tych informacji. Na tym etapie należy uwzględnić dane bezpośrednie i techniczne.
- Jak zbieramy dane? – opis czynności, podczas których zostają zbierane dane.
- Jak wykorzystujemy dane? - opis celów związanych z gromadzeniem danych osobowych oraz informacja o udostępnianiu danych podmiotom trzecim.
- Jak przechowujemy dane? – opis zabezpieczeń do ochrony przetwarzanych danych oraz czas przechowywania informacji.
- Marketing – opis dodatkowych serwisów do kampanii marketingowych oraz obowiązek informacyjny „na żądanie".

[64] PARP*, Ochrona danych osobowych. Poradnik dla małych i średnich przedsiębiorców*, PARP druk, Warszawa 2017, s. 32.
[65] M. Błażewski, *Środki prawne…*, op.cit., s. 51.
[66] Guidelines on Transparency under Regulation 2016/679, s.13-22.

- Twoje prawa – informacja o prawach i wolnościach użytkowników oraz ocena ryzyka z tym związanego.
- Przenoszenie danych – informacja o możliwości przeniesienia danych w ramach prawa żądania danych i pobrania raportów zgromadzonych danych o użytkowniku.
- Polityka cookies – czym są ciasteczka; cele ich zbierania i wyszczególnienie typów plików tekstowych które są gromadzone.
- Zmiany w Polityce Prywatności – informacja o poprawkach w umowie; dotyczy bezpośredniego nadzoru nad zgodnością z aktualnymi przepisami o ochronie danych osobowych.
- Dane kontaktowe
- Dane kontaktowe do instytucji regulującej – prawo do zgłaszania skarg dotyczących przetwarzania danych.

Polityka Ochrony Danych Osobowych w Państwowej Straży Pożarnej określa zasady w zakresie zarządzania procesami przetwarzania danych osobowych oraz ich bezpieczeństwem w danej Komendzie. Opracowanie i stosowanie takiej polityki narzucają na instytucje zapisy art. 24 ust. 2 i art. 32 ust. 2 ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016 r. Parlamentu Europejskiego i Rady (UE) 2016/679 z uwzględnieniem opinii zawartej w motywie 78 tego rozporządzenia oraz ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych.

Na podstawie przytoczonych przepisów Komendant Główny PSP wydał wytyczne z dnia 18 lutego 2020 r. w sprawie organizacji ochrony danych osobowych w jednostkach organizacyjnych Państwowej Straży Pożarnej.

Polityka ma zastosowanie do:

1) danych osobowych przetwarzanych w Komendzie niezależnie od sposobu ich utrwalenia,
2) danych osobowych przetwarzanych, zarówno w zbiorach jak i w formie nieuporządkowanej w zestawach, jak i pojedynczych informacji osobowych,
3) informacji, dotyczących bezpieczeństwa danych osobowych, w szczególności identyfikatorów i haseł we wszystkich systemach/aplikacjach,
4) informacji zawartych w rejestrach, instrukcjach i procedurach związanych z przetwarzaniem lub ochroną danych osobowych.

Za przetwarzanie i ochronę danych osobowych w Komendzie odpowiedzialny jest Administrator Danych Osobowych. Administratorem w rozumieniu art. 4 pkt. 1) RODO jest

dany kierownik jednostki organizacyjnej. W sytuacjach szczególnych Administrator może w formie odrębnego aktu wewnętrznego takiego jak rozkaz, zarządzenie, decyzja doprecyzować postanowienia polityki ochrony danych osobowych. Doprecyzowanie to powinno być poprzedzone konsultacjami z inspektorem ochrony danych, a w sytuacji dotyczącej bezpośrednio systemu informatycznego także z administratorem systemu informatycznego. Inspektor ochrony danych to osoba wyznaczona przez administratora komendy wojewódzkiej i zajmująca samodzielne stanowisko ds. ochrony danych osobowych, realizująca zadania, o których mowa w art. 39 ust. 1 RODO.

Natomiast administrator systemu informatycznego to funkcjonariusz wyznaczony przez Komendanta, odpowiedzialny za nadzór nad zabezpieczeniem i odpowiednim funkcjonowaniem systemów informatycznych, w których przetwarzane są dane osobowe w komendzie. Pełni on również funkcję administratora aplikacji/systemów, w których są przetwarzane dane osobowe, Jest to osoba odpowiedzialna za realizację zabezpieczeń i odpowiednie funkcjonowanie systemów informatycznych, w których przetwarzane są dane osobowe.

W każdej komendzie prowadzony jest rejestr czynności przetwarzania danych osobowych, na których przetwarzanie wyraził zgodę i określił cele Administrator. Rejestr czynności przetwarzania musi zawierać wszystkie informacje wymagane art. 30 ustęp 1 RODO. Przetwarzanie danych osobowych, które nie zostały ujęte w rejestrze odbywa się bez zgody Administratora i stanowi incydent bezpieczeństwa danych osobowych, za który odpowiada kierownik komórki organizacyjnej – kierownik sekcji, naczelnik wydziału lub osoba zatrudniona na jednoosobowym stanowisku pracy, zgodnie ze strukturą organizacyjną danej komendy, określoną w Regulaminie Organizacyjnym. Dodanie nowej czynności przetwarzania danych osobowych do rejestru wymaga zgody administratora, poprzez skierowany do niego wniosek. W sytuacji akceptacji administratora na rozpoczęcie przetwarzania danych osobowych w związku z nowym celem, kierownik komórki organizacyjnej jest zobowiązany dokonać aktualizacji rejestru czynności przetwarzania.

W przypadku zawarcia umowy powierzenia obejmującą zbiory danych osobowych, dla których podmiotem przetwarzającym jest kierownik jednostki organizacyjnej, prowadzi się rejestr wszystkich kategorii czynności przetwarzania, który musi zawierać wszystkie informacje wymagane art. 30 ustęp 2 RODO.

Dopuszcza się rozbudowywanie rejestrów o kolejne dodatkowe elementy, które traktowane są jako środki organizacyjne mające na celu ochronę praw i wolności osób, których dane dotyczą.

W każdej komendzie prowadzi się również „Rejestr naruszeń ochrony danych osobowych", zgodny ze wzorem określonym przez Komendanta Głównego.

W celu usprawnienia realizacji zadań przypisanych dla administratora, wyznacza on co najmniej jedną osobę wspierającą i posiadającą wiedzę oraz doświadczenie w zagadnieniach ochrony danych osobowych – specjalistę ochrony danych o czym powiadamia właściwy organ nadzorczy. Administrator zapewnia, by osoba taka była właściwie i niezwłocznie włączana we wszystkie sprawy dotyczące ochrony danych osobowych związane z realizacją jego zadań wynikających z RODO. Specjalista ochrony danych osobowych wykonuje zadania w określone w art. 39 RODO oraz w Wytycznych Komendanta Głównego Państwowej Straży Pożarnej w sprawie organizacji ochrony danych osobowych w jednostkach organizacyjnych Państwowej Straży Pożarnej.

Do zadań specjalisty ochrony danych należy, w szczególności:

a) organizacja i udział w opracowywaniu analizy ryzyka naruszenia praw i wolności osób fizycznych oraz organizacja innych działań z zakresu ochrony danych osobowych określonych w przepisach i wskazanych przez administratora;
b) prowadzenie, zgodnie z określonymi wzorami rejestrów wymienionych w polityce ochrony danych osobowych;
c) współpraca z inspektorem ochrony danych osobowych w zakresie realizacji jego obowiązków i obowiązków administratora;
d) współpraca z kierownikami komórek organizacyjnych w sprawach związanych z realizacją praw osób, których dane dotyczą, a także w sprawach związanych z przetwarzaniem danych osobowych;
e) udział w działaniach monitorujących przetwarzanie danych osobowych;
f) organizacja i prowadzenie szkoleń;
g) podejmowania działań, zgodnie z przepisami i obowiązującymi w danej komendzie procedurami, w sytuacji naruszenia ochrony danych osobowych.

Koordynuje on zadania realizowane przez poszczególne komórki organizacyjne, wykonuje wskazane przez administratora określone w RODO oraz polityce ochrony danych. Może także w ramach udzielonego pełnomocnictwa nadzorować realizację zadań przez inne komórki organizacyjne.

Administrator zobowiązany jest do zapewnienia możliwość podnoszenia kwalifikacji wyznaczonemu pracownikowi w zakresie wykonywanych zadań oraz ciągłość jego działania, w szczególności poprzez wyznaczenie osoby zastępującej.

W celu wsparcia działań ochrony danych administrator powołuje Forum Bezpieczeństwa Informacji odpowiedzialne za koordynację wszystkich działań związanych z zapewnieniem bezpieczeństwa informacji w komendzie.

Kierownicy komórek organizacyjnych są odpowiedzialni za zarządzanie procesami przetwarzania i ochrony danych osobowych w podległych komórkach organizacyjnych. Do ich obowiązków, w zakresie zarządzania procesami przetwarzania i ochrony danych osobowych, należy w szczególności:

a) zarządzanie zasobem danych osobowych w ramach zadań, realizowanych przez podległą komórkę organizacyjną;

b) nadzór nad ochroną danych osobowych w podległej komórce organizacyjnej;

c) dopilnowanie, aby terminowo i zgodnie z właściwością, włączać SOD/FBI we wszystkie kwestie dotyczące ochrony danych osobowych;

d) dopuszczanie do przetwarzania danych osobowych w podległej komórce organizacyjnej tylko osób posiadających:

- stosowne przeszkolenie,
- upoważnienie do przetwarzania danych osobowych wydane przez Administratora,
- podpisane oświadczenie o poufności;

e) występowanie z wnioskiem do administratora systemu informatycznego o nadanie, zmianę lub cofnięcie uprawnień do określonego zasobu danych osobowych przetwarzanych w systemie informatycznym, zgodnie z zakresem upoważnienia do przetwarzania danych osobowych, w sposób określony w „Instrukcji Zarządzania Systemem Informatycznym”;

f) Ustalanie z administratorem zamiaru przetwarzania nowych kategorii danych osobowych, utworzenia nowego zbioru, zasobów danych osobowych lub dokonania zmian w obrębie już przetwarzanych; zgłaszanie faktu dokonanych ustaleń do SOD/FBI celem opiniowania i odnotowania ich w określonych rejestrach;

g) ustalanie w porozumieniu z administratorem systemu informatycznego zasad tworzenia kopii zapasowych plików z danymi osobowymi, znajdującymi się na stacjach roboczych użytkowników w podległej komórce organizacyjnej;

h) realizacja procesu udostępniania danych osobowych;

i) realizacja procesu związanego z zapewnieniem praw osobom, których dane dotyczą;

j) realizacja procesu powierzania czynności, związanych z przetwarzaniem danych osobowych innym podmiotom, w tym przygotowanie umów związanych z powierzeniem przetwarzania danych osobowych podmiotowi przetwarzającemu;

k) przedkładanie administratorowi projektów umów związanych z powierzeniem danych osobowych w celu ich zatwierdzenia i podpisania;

l) opracowywanie klauzul informacyjnych, oświadczeń zgody na przetwarzanie danych osobowych, które powinny być stosowane przy zbieraniu danych osobowych w podległej mu komórce organizacyjnej oraz odpowiadanie za ich stosowanie;

m) umożliwienie IOD przeprowadzenia czynności monitorujących określonych w RODO;

n) wykonywanie innych zadań zgodnie z zapisami polityki ochrony danych osobowych.

Za zabezpieczenie techniczne danych osobowych przetwarzanych w systemie informatycznym odpowiada administrator systemu informatycznego, który współpracuje ze specjalistą ochrony danych w zakresie realizacji jego obowiązków w Komendzie. Jest on odpowiedzialny za realizację zabezpieczeń i odpowiednie funkcjonowanie systemów informatycznych, w których przetwarzane są dane osobowe. Decyzję o wyznaczeniu administratora systemu informatycznego podejmuje administrator spośród osób pracujących w komórce organizacyjnej, gdzie funkcjonuje system/aplikacja dziedzinowa.

Zagadnienia związane z bezpieczeństwem teleinformatycznym szczegółowo reguluje „Instrukcja Zarządzania Systemem Informatycznym".

Do obowiązków pracowników i innych osób, takich jak stażyści, praktykanci, członkowie zespołów i komisji powołanych przez administratora, osób realizujących zadania na podstawie umowy cywilno-prawnej, przetwarzających dane osobowe należy:

a) uczestniczenie w szkoleniach z zakresu ochrony danych osobowych organizowanych przez administratora;

b) przetwarzanie tylko tych zasobów danych osobowych, które wynikają z upoważnienia do przetwarzania danych osobowych;

c) przetwarzanie danych osobowych i ich zabezpieczanie z zachowaniem wszelkich zasad bezpieczeństwa wynikających z właściwych przepisów w zakresie ochrony danych osobowych, RODO, Polityki i innych procedur i instrukcji obowiązujących na terenie Komendy, zasad dobrej praktyki;

d) niezwłoczne informowanie administratora o sytuacjach podejrzenia naruszenia ochrony danych osobowych, a także wstrzymanie się wtedy od pracy związanej z przetwarzaniem danych osobowych do czasu zapewnienia bezpieczeństwa;
e) wykonywanie innych czynności zgodnie z zapisami polityki ochrony danych osobowych.

Administrator jest upoważniony do przetwarzania wszelkich danych osobowych, występujących w zasobach danej komendy. Administrator upoważnia osoby zatrudnione w Komendzie bez względu na charakter zatrudnienia, odbywające staż lub praktykę, realizujące zadania na podstawie umowy cywilnoprawnej, realizujące zadania w ramach prac w komisjach, zespołach, grupach roboczych realizujące zadania w ramach służby dyżurnej podczas szkoleń lub w stanowisku kierowania, do przetwarzania danych osobowych w zakresie niezbędnym do realizacji zadań podczas wykonywanej pracy lub innych czynności. Osoby, które nie zostały upoważnione do przetwarzania danych osobowych nie mogą przetwarzać danych osobowych. Upoważnianie wskazanych osób do przetwarzania danych osobowych powinno być poprzedzone szkoleniem. Upoważnienie do przetwarzania danych osobowych dla osób zatrudnionych w Komendzie bez względu na charakter zatrudnienia, odbywających staż lub praktykę, realizujących zadania na podstawie umowy cywilnoprawnej, poza sytuacjami szczególnymi określonymi przez administratora, powinno mieć charakter pisemny. Upoważnianie do przetwarzania danych osobowych osób realizujących zadania w ramach prac w komisjach, zespołach, grupach roboczych, osób realizujących zadania w ramach służby dyżurnej podczas szkoleń lub w stanowisku kierowania, odbywa się w formie rozkazu, zarządzenia, decyzji lub innego aktu. Akt ten powinien wskazywać zakres oraz czasookres nadania i ustania upoważnienia do przetwarzania danych osobowych. Administrator może pisemnie upoważnić inną osobę do nadawania i podpisywania upoważnień do przetwarzania danych osobowych.

Osoby upoważnione do przetwarzania danych osobowych, wraz z nadaniem im upoważnienia do przetwarzania danych osobowych, składają w wydziale właściwym w sprawach kadrowych upoważnienie i oświadczenie osoby upoważnionej o zachowaniu w tajemnicy danych osobowych i sposobów ich zabezpieczenia.

Upoważnienie do przetwarzania danych osobowych wygasa automatycznie wraz z ustaniem stosunku zatrudnienia, zakończeniem wykonywania prac, określonych umową cywilnoprawną / o staż / praktykę, a także obowiązków związanych z pracą w komisjach, zespołach, grupach roboczych, oraz realizowanych w ramach służby dyżurnej podczas

szkoleń lub w stanowisku kierowania. Upoważnienia to administrator może cofnąć o każdym czasie.

Zlecanie jakichkolwiek czynności, związanych z przetwarzaniem danych osobowych podmiotom przetwarzającemu, jest formą powierzenia przetwarzania danych osobowych. Decyzję o powierzeniu przetwarzania danych osobowych podejmuje administrator lub osoba przez niego upoważniona do zawierania umów. Powierzenie przetwarzania danych osobowych odbywa się na podstawie umowy.

Dane osobowe w utworzonych zbiorach muszą być zbierane dla oznaczonych, zgodnych z prawem celów i nie poddawane dalszemu przetwarzaniu niezgodnemu z tymi celami. Zbierane dane osobowe muszą być merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane. Zabronione jest zbieranie wszelkich danych nieistotnych, niemających znaczenia, o większym stopniu szczegółowości niż wynika to z określonego celu. Zabronione jest przetwarzanie danych osobowych, dla których zakres, cel przetwarzania i sposoby przetwarzania nie został ustalony przez administratora, z wyjątkiem danych osobowych wynikających wprost z przepisów prawa. Dane mogą być przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania. Okres przechowywania może zostać wydłużony nawet po osiągnięciu celu przetwarzania, jeżeli przepisy ustaw szczególnych takie postępowanie dopuszczają.

W sytuacji gdy podstawą prawną przetwarzania danych osobowych nie będzie żaden z zapisów art. 6 ust. 1 lit. b),c),d),e) RODO przetwarzanie jest możliwe na podstawie zgody na przetwarzanie danych osobowych wyrażonej przez osobę, której dane dotyczą. Zgoda powinna być wyrażona w drodze jednoznacznej, potwierdzającej czynności, która wyraża odnoszące się do określonej sytuacji dobrowolne, świadome i jednoznaczne przyzwolenie osoby, których dane dotyczą, na przetwarzanie dotyczących jej danych osobowych. Zgoda może mieć formę pisemnego (w tym elektronicznego) lub ustnego oświadczenia. Zgoda na przetwarzanie danych osobowych, która jest częścią składową kwestionariuszy, formularzy, itp., powinna być odebrana (podpisana) odrębnie. W sytuacjach szczególnych, określonych przez administratora, zgoda może być odebrana w formie jednoznacznego, wyraźnego działania.

Kierownik komórki organizacyjnej odpowiedzialny za przetwarzanie danych osobowych do danego celu realizowanego w oparciu o zgodę osoby, której dane dotyczą, zobowiązany jest prowadzić i zarządzać rejestrem bieżących zgód na przetwarzanie danych osobowych.

W przypadku zbierania danych osobowych bezpośrednio od osób - na formularzach, kwestionariuszach, drukach i innych służących do zbierania danych osobowych – prowadzonych zarówno w formie papierowej, jak i elektronicznej, należy umieszczać na nich klauzulę informacyjną.

W przypadku wykorzystania danych osobowych w innym celu niż cel pierwotny, kierownik komórki organizacyjnej zobowiązany jest dokonać aktualizacji klauzuli informacyjnej i dokonać ponownego informowania osób, których dane osobowe zostały zebrane. Możliwe jest odstąpienie od ww. obowiązku, gdy zmiana celu przetwarzania służy realizacji zadania publicznego i niewykonanie obowiązku jest niezbędne dla realizacji celów publicznych, o których mowa w art. 23 ust. 1 RODO oraz przekazanie tych informacji:

a) uniemożliwi lub znacząco utrudni prawidłowe wykonanie zadania publicznego, a interes lub podstawowe prawa lub wolności osoby, której dane dotyczą, nie są nadrzędne w stosunku do interesu wynikającego z realizacji tego zadania publicznego lub;
b) naruszy ochronę informacji niejawnych.

W przypadku pozyskiwania danych osobowych w inny sposób niż od osoby, której dane osobowe dotyczą, administrator jest zobowiązany realizować obowiązek informacyjny w stosunku do tych osób w sposób określony w art. 14 RODO.

Wnioski w sprawie skorzystania z praw osoby, której dane osobowe dotyczą w imieniu Administratora rozpatruje i realizuje właściwy KKO. W przypadku wątpliwości co do zgodności z prawem przyjętego postępowania, a w szczególności w sytuacji wątpliwości do odpowiedzi odmownej lub udostępniania danych, KKO na polecenie Administratora może zasięgnąć opinii IOD. Wnioski o realizację praw osoby, której dane dotyczą rejestruje się „Rejestrze działań w zakresie udostępnień oraz praw osoby, której dane dotyczą", prowadzonym w każdej komórce organizacyjnej dla danych przez nią przetwarzanych. Działania te mogą być także dokumentowane w postaci papierowej lub elektronicznej.

W celu ułatwienia korzystania z praw przez osobę, której dane dotyczą Administrator umożliwia jej kontakt z IOD poprzez umieszczenie kontaktu do niego na stronie internetowej. Przed podjęciem działań związanych z wykonywaniem praw osoby, której dane dotyczą, w pierwszej kolejności należy dokonać autoryzacji osoby, celem bezspornego ustalenia czy osoba, która składa wniosek jest osobą uprawnioną. W przypadku skontaktowania się osoby, której dane dotyczą bezpośrednio z IOD, Administrator lub wskazani przez niego KKO są zobowiązani niezwłocznie udzielić mu wszelkiej możliwej pomocy i informacji w celu ustalenia, która komórka organizacyjna jest odpowiedzialna za rozwią-

zanie problemu oraz spowodowanie, aby osoba, której dane dotyczą mogła skorzystać ze swoich praw.

Odpowiedź na każde zgłoszone żądanie realizacji prawa bez zbędnej zwłoki, jednakże nie później niż w terminie miesiąca od dnia otrzymania danego żądania. Odpowiedzi udziela się w tej samej formie, w której żądanie zostało zgłoszone, chyba że Osoba, której dane dotyczą, zażąda udzielenia odpowiedzi w innej formie. W wyjątkowych sytuacjach, tj. z uwagi na skomplikowany charakter żądania lub liczbę żądań w danym okresie, Administrator jest uprawniony do przedłużenia terminu realizacji żądania o kolejne dwa miesiące. W takim przypadku informuje on o tym Osobę, której dane dotyczą, nie później niż w terminie jednego miesiąca od dnia otrzymania żądania, z podaniem przyczyny przedłużenia.

W przypadku gdy nie ma podstaw do realizacji żądania Osoby, której dane dotyczą, osoba odpowiedzialna informuje o tym Osobę, której dane dotyczą, wskazując powody niepodejmowania działań oraz informując o możliwości wniesienia skargi do organu nadzorczego oraz skorzystania ze środków ochrony prawnej przed sądem.

KKO informuje o sprostowaniu, uzupełnieniu, usunięciu lub ograniczeniu przetwarzania danych osobowych każdego odbiorcę, któremu ujawniono dane osobowe, chyba że byłoby to niemożliwe lub wymagające niewspółmiernie dużego wysiłku. W przypadku zaistnienia któregokolwiek z tych wyjątków, KKO sporządza notatkę ze stosownym uzasadnieniem i przedkłada ją Administratorowi.

Dane osobowe mogą być udostępniane w następujących przypadkach:

a) na podstawie przepisów prawa organom publicznym w ramach konkretnego postępowania,
b) na podstawie wniosku od podmiotu uprawnionego do otrzymania danych na podstawie przepisów prawa,
c) na podstawie umowy z odbiorcą danych lub współadministratorem danych, w ramach której istnieje konieczność udostępnienia danych.

Proces udostępniania danych osobowych rozpatruje i realizuje właściwy KKO; w przypadku wątpliwości co do zgodności z prawem przyjętego postępowania, KKO na polecenie Administratora może zasięgnąć opinii IOD.

Informacje zawierające dane osobowe, przekazywane są uprawnionym podmiotom lub osobom, za potwierdzeniem odbioru, w następujący sposób:

a) pocztą kurierską,

b) listem poleconym za pokwitowaniem odbioru,
c) za pomocą teletransmisji danych,
d) osobiście za potwierdzeniem odbioru.
e) w inny, określony konkretnym wymogiem prawnym lub umową, sposób.

Administrator systemu informatycznego nadzoruje przestrzeganie zasad bezpieczeństwa, w przypadku udostępniania danych osobowych drogą elektroniczną.

Osoby przetwarzające dane osobowe zachowują szczególną ostrożność przy przekazywaniu danych osobowych drogą telefoniczną; przekazanie tą drogą może nastąpić tylko w sytuacji pełnej pewności co do tożsamości osoby, której dane są przekazywane.

Każda osoba fizyczna ma prawo zgłoszenia żądania uzyskania od Administratora informacji, czy Administrator przetwarza jej dane osobowe, a jeśli tak, ma prawo żądania uzyskania dostępu do tych danych oraz informacji, o których mowa art. 15 RODO, tj.:

a) cele przetwarzania;
b) kategorie odnośnych danych osobowych;
c) informacje o odbiorcach lub kategoriach odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w szczególności o odbiorcach w państwach trzecich lub organizacjach międzynarodowych;
d) w miarę możliwości planowany okres przechowywania danych osobowych, a gdy nie jest to możliwe, kryteria ustalania tego okresu;
e) informacje o prawie do żądania od administratora sprostowania, usunięcia lub ograniczenia przetwarzania danych osobowych dotyczącego Osoby, której dane dotyczą, oraz do wniesienia sprzeciwu wobec takiego przetwarzania;
f) informacje o prawie wniesienia skargi do organu nadzorczego;
g) jeżeli dane osobowe nie zostały zebrane od osoby, której dane dotyczą – wszelkie dostępne informacje o ich źródle;
h) informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, o którym mowa w art. 22 ust. 1 i 4 RODO, oraz – przynajmniej w tych przypadkach – istotne informacje o zasadach ich podejmowania,

Administrator, na żądanie Osoby, której dane dotyczą, dostarcza jej również kopię danych osobowych podlegających przetwarzaniu.

Jeżeli dane osobowe są przekazywane do państwa trzeciego lub organizacji międzynarodowej, Osoba, której dane dotyczą, ma prawo zostać poinformowana o odpowiednich zabezpieczeniach, o których mowa w art. 46 RODO, związanych z przekazaniem.

Każda Osoba, której dane dotyczą, ma prawo żądania od Administratora sprostowania dotyczących jej danych osobowych, które są nieprawidłowe. Z uwzględnieniem celów przetwarzania, Osoba, której dane dotyczą, ma prawo żądania uzupełnienia niekompletnych danych osobowych. Administrator dokonuje sprostowania lub uzupełnienia w sposób odpowiadający okolicznościom danego procesu przetwarzania, np. poprzez przedstawienie Osobie, której dane dotyczą, dodatkowego formularza do wypełnienia. Administrator informuje o sprostowaniu lub usunięciu danych osobowych lub ograniczeniu przetwarzania, których dokonał zgodnie z art. 16 RODO (prawo do sprostowania danych), art. 17 ust. 1 RODO (prawo do usunięcia danych) i art. 18 RODO (prawo do ograniczenia przetwarzania), każdego odbiorcę, któremu ujawniono dane osobowe, chyba że okaże się to niemożliwe lub będzie wymagać niewspółmiernie dużego wysiłku. Administrator informuje Osobę, której dane dotyczą, o tych odbiorcach, jeżeli Osoba, której dane dotyczą, tego zażąda.

Każda Osoba, której dane dotyczą, ma prawo żądania od Administratora usunięcia dotyczących jej danych osobowych, jeżeli zachodzi jedna z następujących okoliczności:

a) dane osobowe nie są już niezbędne do celów, w których zostały zebrane lub w inny sposób przetwarzane;
b) Osoba, której dane dotyczą, cofnęła zgodę będąca podstawą do przetwarzania danych zgodnie z art. 6 ust. 1 lit. a) RODO, a brak jest innej podstawy przetwarzania;
c) Osoba, której dane dotyczą, wniosła sprzeciw wobec przetwarzania danych osobowych;
d) dane osobowe są przetwarzane niezgodnie z prawem;
e) dane osobowe muszą zostać usunięte w celu wywiązania się z obowiązku prawnego przewidzianego w prawie Unii Europejskiej lub prawie polskim;
f) dane osobowe zostały zebrane w związku z oferowaniem usług społeczeństwa informacyjnego oferowanych bezpośrednio dziecku.

Każda Osoba, której dane dotyczą ma prawo żądania od Administratora ograniczenia przetwarzania jej danych osobowych, w przypadku, gdy:

a) kwestionuje ona prawidłowość danych osobowych – na okres pozwalający Administratorowi sprawdzić prawidłowość tych danych;
b) przetwarzanie jest niezgodne z prawem, a Osoba sprzeciwia się usunięciu danych osobowych, żądając w zamian ograniczenia ich wykorzystywania;
c) Administrator nie potrzebuje już danych osobowych do celów przetwarzania, ale są one potrzebne Osobie do ustalenia, dochodzenia lub obrony roszczeń;

d) Osoba, której dane dotyczą wniosła sprzeciw wobec przetwarzania danych – do czasu stwierdzenia, czy prawnie uzasadnione podstawy po stronie Administratora są nadrzędne wobec podstaw sprzeciwu.

W przypadku wykonania żądania realizacji prawa, o którym mowa powyżej, Administrator dokonuje oznaczenia danych objętych żądaniem i zaprzestaje ich przetwarzania w inny sposób niż ich przechowywanie, chyba że:

a) Osoba, której dane dotyczą, wyrazi zgodę na inny sposób przetwarzania danych,

b) jest to niezbędne w celu ustalenia, dochodzenia lub obrony roszczeń,

c) jest niezbędne w celu ochrony praw innej osoby fizycznej lub prawnej,

d) z uwagi na ważne względy interesu publicznego Unii Europejskiej lub państwa członkowskiego.

W przypadku uchylenia ograniczenia przetwarzania danych osobowych, Administrator informuje o tym Osobę, której dane dotyczą.

Każda Osoba, której dane dotyczą, ma prawo wnieść sprzeciw – z przyczyn związanych z jej szczególną sytuacją – w przypadku gdy Administrator przetwarza dane na następujących podstawach:

a) przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej Administratorowi;

b) przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez Administratora lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności Osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności gdy Osoba, której dane dotyczą, jest dzieckiem;

c) w tym profilowania na podstawie przepisów art. 6 ust.1 lit. e) i f) RODO wymienionych powyżej w punktach a) oraz b).

Nie dotyczy sytuacji, gdy istnieją ważne, prawnie uzasadnione podstawy do przetwarzania, nadrzędne wobec interesów, praw i wolności Osoby, której dane dotyczą lub podstawy do ustalenia, dochodzenia lub obrony roszczeń. W przypadku zaistnienia którejkolwiek z tych okoliczności, Inspektor sporządza stosowną notatkę z uzasadnieniem.

Każda Osoba, której dane dotyczą, ma prawo wnieść sprzeciw w przypadku, gdy jej dane osobowe są przetwarzane na potrzeby marketingu bezpośredniego w zakresie, w jakim przetwarzanie jest związane z takim marketingiem bezpośrednim.

Każda Osoba, której dane dotyczą, ma prawo otrzymać w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego dane osobowe jej dotyczące, które dostarczyła Administratorowi, oraz ma prawo przesłać te dane osobowe innemu administratorowi bez przeszkód ze strony Administratora, jeżeli:
a) przetwarzanie odbywa się na podstawie zgody lub na podstawie niezbędności do wykonania umowy, której stroną jest Osoba, której dane dotyczą, lub do podjęcia działań na żądanie tej Osoby przed zawarciem umowy, oraz
b) przetwarzanie odbywa się w sposób zautomatyzowany.
Jeżeli jest to technicznie możliwe, na żądanie Osoby, której dane dotyczą, Administrator przesyła dane bezpośrednio innemu administratorowi.

Obszarem przetwarzania danych osobowych w Komendzie są budynki, pomieszczenia lub części pomieszczeń, w których są przetwarzane dane osobowe zarówno w formie papierowej, jak i w systemie informatycznym.
Przebywanie wewnątrz obszaru przetwarzania danych osobowych, osób nieuprawnionych do dostępu do danych osobowych - jest dopuszczalne za zgodą Administratora lub w obecności osoby dopuszczonej do przetwarzania tych.
Pracownicy firm zewnętrznych, przebywający wewnątrz obszaru przetwarzania danych osobowych poza godzinami pracy lub bez obecności osoby dopuszczonej do przetwarzania danych powinny podpisać oświadczenia, o których mowa w § 15 PODO i powinny one być dołączone do umów z tymi firmami.
Pomieszczenia, w których przetwarzane są dane osobowe, powinny być zamykane na czas nieobecności w nich osób dopuszczonych do danych osobowych, w sposób uniemożliwiający dostęp do nich osobom nieupoważnionym.
Niedopuszczalne jest wynoszenie materiałów zawierających dane osobowe poza obszar ich przetwarzania bez związku z wykonywaniem czynności służbowych.
Za bezpieczeństwo i zwrot materiałów zawierających dane osobowe odpowiada osoba dokonująca ich wyniesienia.
W przypadku wątpliwości co do przetwarzania danych osobowych poza obszarem ich przetwarzania, KKO na polecenie administratora może zasięgnąć opinii SOD.

Dane osobowe, zawarte w dokumentacji papierowej, mogą być przetwarzane jedynie przez osoby upoważnione do przetwarzania danych osobowych zgodnie z zasadami określonymi w PODO. Kopie papierowe z danymi osobowymi muszą być przechowywane

w zamykanych na klucz szafach, szufladach lub sejfach; obowiązuje tzw. „zasada czystego biurka".

Dopuszcza się przechowywanie danych osobowych w niezamykanych szafach lub regałach tylko w pomieszczeniu archiwum zabezpieczonym zgodnie z odrębnymi przepisami.

Niszczenie dokumentów papierowych powinno przebiegać z wykorzystaniem specjalnych urządzeń do wykonywania tych czynności takich jak niszczarki.

Zasady przechowywania, sposób archiwizowania i likwidacji dokumentów papierowych, określają przepisy kancelaryjne Komendy. W zakresie nieuregulowanym przepisami kancelaryjnymi Komendy, odpowiednie zasady określa KKO po konsultacji z Administratorem; w sytuacjach szczególnych mogą w tej sprawie zasięgnąć porady SOD.

Oczywiście w polityce ochrony danych osobowych Państwowej Straży pożarnej unormowane zostało postępowanie w sytuacji naruszenia ochrony danych osobowych. Każdy pracownik zobowiązany do ochrony danych osobowych jeśli stwierdzi lub podejrzewa naruszenie zabezpieczenia danych osobowych, powinien niezwłocznie poinformować o tym:

a) właściwego KKO, którego obowiązkiem jest poinformowanie o naruszeniu Administratora lub osoby zastępującej KJO oraz SOD, ASI (jeśli naruszenie dotyczy systemów informatycznych);
b) bezpośrednio Administratora w sytuacjach szczególnych, do których zaliczyć można podejrzenie braku bezstronności osób wskazanych w powyższym punkcie.

Informację o naruszeniu Administrator powinien niezwłocznie przekazać do SOD w celu umożliwienia mu realizacji jego obowiązków.

Ponadto każdy kto stwierdził lub podejrzewa naruszenie zabezpieczenia danych osobowych, oprócz obowiązku wymienionego powyżej powinien:

a) powstrzymać się od wykonywania pracy lub jakichkolwiek czynności mogących spowodować zatarcie śladów lub dowodów naruszenia;
b) podjąć, odpowiednie do zaistniałej sytuacji działania niezbędne do zapobieżenia dalszym zagrożeniom, które mogą skutkować naruszeniem danych osobowych.

Administrator, a w przypadku jego nieobecności osoba wyznaczona przez KJO, po stwierdzeniu lub uzyskaniu informacji o naruszeniu ochrony danych osobowych powinien:

a) przystąpić do identyfikacji rodzaju zdarzenia, a w szczególności do określenia skali zniszczeń, dostępu do danych osobowych itp., W tym zakresie niezbędne może okazać się zebranie pisemnych wyjaśnień od osób odpowiedzialnych. Ważnym elementem

identyfikacji naruszenia jest sporządzenie „Analizy wystąpienia ryzyka naruszenia praw lub wolności w związku z incydentem ochrony danych osobowych". Analizę sporządza wyznaczony przez Administratora SOD lub KKO, względnie ASI dla systemów informatycznych. Analiza podlega opiniowaniu przez IOD.

b) podjąć odpowiednie kroki w celu zminimalizowania szkód i rozmiarów zdarzenia oraz zabezpieczenia przed usunięciem śladów zdarzenia;
c) osobiście lub polecić SOD lub KKO w terminie 72 godzin przesłać do właściwego Organu Nadzorczego zgłoszenie naruszenia ochrony danych osobowych jeżeli skutkowało ono ryzykiem naruszenia praw i wolności osób fizycznych; Sposób zgłaszania o naruszeniach został opisany na stronie Urzędu Ochrony Danych Osobowych znajdujący się pod adresem https://uodo.gov.pl/pl/134/233;
d) osobiście lub polecić SOD lub KKO bez zbędnej zwłoki zawiadomić osobę, której dane dotyczą o naruszeniu jeżeli skutkowało ono ryzykiem naruszenia praw i wolności osób fizycznych; postępowanie to powinno być zgodne z art. 34 RODO;
e) zgłoszenie i powiadomienie, przekazać do wiadomości IOD, a także wszelkie niezbędne informacje do realizacji jego obowiązków;

SOD jest zobowiązany zarejestrować zdarzenie zgodnie z „Rejestrem naruszeń ochrony danych osobowych"

Administrator w sytuacjach szczególnych, takich jak konieczność zgłoszenia naruszenia ochrony danych osobowych do właściwego Organu Nadzorczego, dokumentuje podejmowane działania. Sporządzeniem tej dokumentacji powinien zająć się SOD lub KKO wskazany przez Administratora. Sprawozdanie z okoliczności zdarzenia osoba sporządzająca przedkłada KJO, po zaopiniowaniu przez IOD.

W przypadku zdarzenia mającego związek z systemem informatycznym ABI zobowiązany jest do:

a) szczegółowej analizy systemu w celu potwierdzenia lub wykluczenia faktu naruszenia,
b) wygenerowania, wydrukowania wszystkich możliwych dokumentów, raportów lub zestawień, które mogą pomóc w ustaleniu okoliczności zdarzenia, opatrując je datą i podpisem,
c) fizycznego odłączenia urządzenia, segmentu sieci, które mogły umożliwiać dostęp do bazy danych osobowych osobie nieupoważnionej,
d) wylogowania użytkownika podejrzewanego o naruszenie ochrony danych osobowych,
e) zmiany haseł na konta, poprzez które uzyskano nielegalny dostęp,

f) przywrócenia normalnego działania systemu, przy czym, jeżeli nastąpiło uszkodzenie bazy danych, przywrócenia jej z ostatniej kopii awaryjnej z zachowaniem środków ostrożności przed ponownym dostępem tą samą drogą przez osobę nieupoważnioną.

ABI o podjętych działaniach powinien niezwłocznie poinformować Administratora.
Wszyscy zobowiązani mają obowiązek udzielić wszelkiej niezbędnej pomocy przy realizacji zadań przez SOD i ABI.

Oprócz polityki ochrony danych osobowych w Państwowej Straży Pożarnej funkcjonuje ochrona informacji niejawnych. Ma to odniesienie do funkcjonującego w Rzeczypospolitej Polskiej systemu ochrony informacji, których bezprawne ujawnienie mogłoby zaszkodzić naszemu państwu lub jego interesom. Główną podstawą prawną, regulującą założenia o informacjach niejawnych jest Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych. Informacja niejawna według polskiej ustawy o ochronie informacji niejawnych jest to informacja, której "nieuprawnione ujawnienie spowodowałoby lub mogłoby spowodować szkody dla Rzeczypospolitej Polskiej albo byłoby z punktu widzenia jej interesów niekorzystne, także w trakcie ich opracowywania oraz niezależnie od formy i sposobu ich wyrażania[67]".
Kwestia ta została uregulowana w art. 4 wyżej wspomnianej ustawy, dostęp do tego typu informacji mogą mieć jedynie osoby, które dają rękojmię zachowania tajemnicy, a informacje te są niezbędne do wykonywania przez te osoby pracy lub pełnienia służby na zajmowanym stanowisku. Można tu zauważyć występowanie zasady wiedzy niezbędnej również zwaną zasadą wiedzy koniecznej[68].

Do języka prawnego pojęcie informacji niejawnej zostało wprowadzone dopiero przepisami ustawy z 1999 o ochronie informacji niejawnych od tego czasu ustawa ulegała kilkukrotnym zmianom[69].
Większe zmiany zostały wprowadzone w ustawie z 2010 roku i miały między innymi następujące skutki:

- Zaprzestano zwrotów takich pojęć jak tajemnica państwowa i tajemnica służbowa, natomiast zmianie nie ulega klasyfikacja informacji niejawnych z podziałem na ściśle tajne, tajne, poufne i zastrzeżone,

[67] Ustawa o ochronie informacji niejawnych 2010, art. 1
[68] S. Zalewski, *Informacje niejawne we współczesnym państwie*, Editions Spotkania, Warszawa, 2017 r., s.57.
[69] R. Szałowski, *Informacje niejawne zagadnienia prawnoadministracyjne*, Wydawnictwo im. Stanisława Podobińskiego Akademii im. Jana Długosza w Częstochowie, Częstochowa 2011 r.,, s. 11.

- Informacje dotyczące prawnie chronionych w odniesieniu do interesów obywateli a także innych jednostek organizacyjnych objętych tajemnicami, których ochrona jest regulowana poprzez inne ustawy przestały być traktowane jako informacje niejawne,
- Dodano możliwość zmiany lub zniesienia danej klauzuli w momencie gdy istniejące przesłanki ochrony ustaną,
- Umieszczono obowiązek przeglądu dokumentów, w celu określenia czy dalej spełniają warunki nadania im odpowiedniej klauzuli tajności.

Odnośnie do samej klasyfikacji informacji niejawnych to kwestia powyższa poruszana jest w art. 5 ustawy o ochronie informacji niejawnych. Odpowiednią klauzulę nadaję się biorąc pod uwagę zagrożenia jakie spowodowałoby ujawnienie danej informacji bez uprawnień. Osoba odpowiedzialna za nadawanie klauzuli to osoba, która ma uprawnienia do podpisania dokumentu lub oznaczenia materiału innego niż dokument.

Poniżej zostaną omówione poszczególne rodzaje informacji niejawnych ze względu na klauzulę tajności[70].

Informacjom niejawnym nadaje się klauzulę ściśle tajne, jeżeli ich nieuprawnione ujawnienie spowoduje wyjątkowo poważną szkodę dla Rzeczypospolitej Polskiej przez to, że[71]:

- zagrozi niepodległości, suwerenności lub integralności terytorialnej Rzeczypospolitej Polskiej,
- zagrozi bezpieczeństwu wewnętrznemu lub porządkowi konstytucyjnemu Rzeczypospolitej Polskiej,
- zagrozi sojuszom lub pozycji międzynarodowej Rzeczypospolitej Polskiej,
- osłabi gotowość obronną Rzeczypospolitej Polskiej,
- doprowadzi lub może doprowadzić do identyfikacji funkcjonariuszy, żołnierzy lub pracowników służb odpowiedzialnych za realizację zadań wywiadu lub kontrwywiadu, którzy wykonują czynności operacyjno-rozpoznawcze, jeżeli zagrozi to bezpieczeństwu wykonywanych czynności lub może doprowadzić do identyfikacji osób udzielających im pomocy w tym zakresie,
- zagrozi lub może zagrozić życiu lub zdrowiu funkcjonariuszy, żołnierzy lub pracowników, którzy wykonują czynności operacyjno-rozpoznawcze, lub osób udzielających im pomocy w tym zakresie, zagrozi lub może zagrozić życiu lub zdrowiu świadków koronnych lub osób dla nich najbliższych, osób, którym udzielono środków ochrony

[70] R. Szałowski, *Informacje*…, op.cit., s 39-40.

[71] Ustawa o ochronie informacji niejawnych (2010), Dz.U. 2018 poz. 412 art. 5.

i pomocy przewidzianych w ustawie z dnia 28 listopada 2014 r. o ochronie i pomocy dla pokrzywdzonego i świadka (Dz. U. z 2015 r. poz. 21), albo świadków, o których mowa w art. 184 ustawy z dnia 6 czerwca 1997 r. – Kodeks postępowania karnego, lub osób dla nich najbliższych.

Informacjom niejawnym nadaje się klauzulę tajne, jeżeli ich nieuprawnione ujawnienie spowoduje poważną szkodę dla Rzeczypospolitej Polskiej przez to, że[72]:

- uniemożliwi realizację zadań związanych z ochroną suwerenności lub porządku konstytucyjnego Rzeczypospolitej Polskiej,
- pogorszy stosunki Rzeczypospolitej Polskiej z innymi państwami lub organizacjami międzynarodowymi,
- zakłóci przygotowania obronne państwa lub funkcjonowanie Sił Zbrojnych Rzeczypospolitej Polskiej,
- utrudni wykonywanie czynności operacyjno-rozpoznawczych prowadzonych w celu zapewnienia bezpieczeństwa państwa lub ścigania sprawców zbrodni przez służby lub instytucje do tego uprawnione,
- w istotny sposób zakłóci funkcjonowanie organów ścigania i wymiaru sprawiedliwości,
- przyniesie stratę znacznych rozmiarów w interesach ekonomicznych Rzeczypospolitej Polskiej.

Informacjom niejawnym nadaje się klauzulę poufne, jeżeli ich nieuprawnione ujawnienie spowoduje szkodę dla Rzeczypospolitej Polskiej przez to, że:

- utrudni prowadzenie bieżącej polityki zagranicznej Rzeczypospolitej Polskiej,
- utrudni realizację przedsięwzięć obronnych lub negatywnie wpłynie na zdolność bojową Sił Zbrojnych Rzeczypospolitej Polskiej,
- zakłóci porządek publiczny lub zagrozi bezpieczeństwu obywateli,
- utrudni wykonywanie zadań służbom lub instytucjom odpowiedzialnym za ochronę bezpieczeństwa lub podstawowych interesów Rzeczypospolitej Polskiej,
- utrudni wykonywanie zadań służbom lub instytucjom odpowiedzialnym za ochronę porządku publicznego, bezpieczeństwa obywateli lub ściganie sprawców przestępstw i przestępstw skarbowych oraz organom wymiaru sprawiedliwości,
- zagrozi stabilności systemu finansowego Rzeczypospolitej Polskiej,
- wpłynie niekorzystnie na funkcjonowanie gospodarki narodowej.

[72] Ibidem, poz.412 art.5.

Informacjom niejawnym nadaje się klauzulę zastrzeżone, jeżeli nie nadano im wyższej klauzuli tajności, a ich nieuprawnione ujawnienie może mieć szkodliwy wpływ na wykonywanie przez organy władzy publicznej lub inne jednostki organizacyjne zadań w zakresie obrony narodowej, polityki zagranicznej, bezpieczeństwa publicznego, przestrzegania praw i wolności obywateli, wymiaru sprawiedliwości albo interesów ekonomicznych Rzeczypospolitej Polskiej[73].

Reasumując powyższe można stwierdzić, że informacje niejawne związane są z:

- czynnikami mającymi wpływ na ochroną bezpieczeństwa państwa,
- obronnością państwa,
- bezpieczeństwem i porządkiem publicznym,
- prowadzoną polityką zagraniczna,
- gospodarką i finansami państwa,
- wymiarem sprawiedliwości,
- sprawnością prowadzenia przez uprawnione służby czynności operacyjnych i rozpoznawczych.

Kolejną niezmiernie istotną kwestią jest okres ochrony jakim są objęte informacje niejawne. Zostało to uregulowane w art. 6 ustawy o ochronie informacji niejawnych, zgodnie z którym kierownicy jednostek organizacyjnych mają obowiązek dokonywania przeglądów materiałów nie rzadziej niż co 5 lat. Ma to na celu ustalenie, czy dalej dokumenty te spełniają ustawowe przesłanki ochrony, wówczas możliwa jest zniesienia lub zmiana klauzuli tajności danej informacji.

Poświadczenie bezpieczeństwa, które upoważnia do dostępu do informacji niejawnych wydaje się w zależności od poziomu klauzuli informacji niejawnych na czas:

- 5 lat – jeżeli dotyczy dostępu do informacji niejawnych o klauzuli "ściśle tajne".
- 7 lat – jeżeli dotyczy dostępu do informacji niejawnych o klauzuli "tajne";
- 10 lat – jeżeli dotyczy dostępu do informacji niejawnych o klauzuli "poufne";

Proces przyznawania uprawnień poprzedza wieloetapowy proces, który szczegółowo jest opisany wart 29 ustawy o ochronie informacji. Aby otrzymać poświadczenie bezpieczeństwa wymagane jest poddanie się postępowaniu sprawdzającemu[74]. Głównym celem przeprowadzenia takiego postępowania jest stwierdzenie, czy osoba ubiegająca się o dostęp do informacji niejawnych daje rękojmię zachowania tajemnicy.

[73] Ustawa o ochronie informacji niejawnych, (2010), Dz.U. 2018 poz. 412 art. 5.

[74] K. Grott, M. Szostak, *Bezpieczeństwo obiegu dokumentów w sądach administracyjnych*, *Przegląd nauk sto*sowanych, 2017 r., nr 17, s. 35.

Występują trzy rodzaje postepowania[75]:

- Postępowanie zwykłe – dotyczy osób ubiegających się o dostęp do dokumentów opatrzonych klauzulą "zastrzeżone" i "poufne"
- Postępowanie poszerzone – dotyczy osób ubiegających się o dostęp do dokumentów opatrzonych klauzulą "tajne"
- Postępowanie specjalne – dotyczy osób ubiegających się o dostęp do dokumentów opatrzonych klauzulą "ściśle tajne"

Postępowanie sprawdzające może posiadać trzy rezultaty: wydanie poświadczenia bezpieczeństwa, odmowę lub umorzenie[76].

W przypadku posiadania poświadczenia bezpieczeństwa, które uprawnia do dostępu do dokumentów o wyższym stopniu klauzuli tajności, ten sam dokument również pozwala na dostęp do dokumentów opatrzonych klauzulą o niższym stopniu tajności.

Piecze nad systemem ochrony informacji niejawnych w Polsce pełni Agencja Bezpieczeństwa Wewnętrznego i Służba Kontrwywiadu Wojskowego. Są to organy odpowiedzialne za:

- kontrole nad ochroną informacji niejawnych
- przestrzeganie przepisów z tego zakresu,
- wykonywanie zadań, które odnoszą się do bezpieczeństwa systemów informatycznych,
- prowadzenie postępowań sprawdzających, kontrolnych postępowań sprawdzających,
- zapewnienie ochrony informacji niejawnych wymienianych pomiędzy Rzeczpospolitą Polską a innymi państwami,
- prowadzenie doradztwa i szkoleń w zakresie i ochrony informacji niejawnych.

W Państwowej Straży Pożarnej ochrona informacji niejawnych realizowana jest przy pomocy wyodrębnionych w każdej komendzie kancelarii tajnych. Są to wyodrębnione komórki organizacyjne w zakresie ochrony informacji niejawnych i podlegają bezpośrednio kierownikowi danej jednostki organizacyjnej. Kancelarie te obsługiwane są przez osoby odpowiedzialne za właściwe rejestrowanie, przechowywanie, obieg i wydawanie materiałów uprawnionym osobom, a następnie ich archiwizowanie. Zadaniem kancelarii tajnych jest przede wszystkim zagwarantowanie sprawnej wymiany informacji pomiędzy

[75] Z. Wróblewski, *Ochrona informacji niejawnych. Zagadnienia ogólne*, Zeszyty Naukowe Państwowej Wyższej Szkoły Zawodowej im. Witelona w Legnicy, Legnica 2008 r., nr 4, s. 111.

[76] M. Karpiuk, *Miejsce bezpieczeństwa osobowego w systemie ochrony informacji niejawnych*, *Studia nad autorytaryzmem i totalitaryzmem,* 2018 r., nr 1, s. 96.

upoważnionymi wykonawcami. Jednocześnie powinny one stanowić fizyczną barierę dostępu do informacji dla osób, które nie posiadają odpowiednich uprawnień[77].

Każdy kierownik jednostki organizacyjnej PSP (komendant), w której przetwarzane są niejawne dane, jest odpowiedzialny za ochronę tych informacji. Głównym jego zadaniem jest zorganizowanie i prawidłowe funkcjonowanie tej ochrony. W jednostce, w której przetwarzane są informacje o klauzuli "tajne" lub "ściśle tajne", kierownik danej jednostki ma obowiązek utworzenia kancelarii tajnej. Fakt utworzenia bądź likwidacji kancelarii tajnej kierownik jednostki organizacyjnej musi zgłosić Służbie Kontrwywiadu Wojskowego oraz jednocześnie określić klauzulę tajności informacji niejawnych, jakie będą w niej przetwarzane. Kierownik jednostki może także udzielać zgody na przetwarzanie w kancelarii tajnej informacji o niższej klauzuli, tj. "zastrzeżone" oraz "poufne".

Kierownik jednostki organizacyjnej akceptuje projekty dokumentów, które przygotowuje dla niego pełnomocnik. W dokumentach tych powinien zostać określony:

- stopień zagrożeń związanych z nieuprawnionym dostępem do informacji niejawnych lub sytuacją, gdy dojdzie do ich utraty,
- tryb i sposób przetwarzania informacji niejawnych o klauzuli "poufne" w komórkach organizacyjnych,
- sposób oraz tryb przetwarzania informacji niejawnych o klauzuli "zastrzeżone", z uwzględnieniem obszaru środków bezpieczeństwa fizycznego w celu ich ochrony,
- forma zabezpieczenia informacji niejawnych w jednostce organizacyjnej.

[77] S. Kaleta, *Rola i znaczenie kancelarii tajnych dla ochrony informacji niejawnych w resorcie obrony narodowej,* Kultura bezpieczeństwa, Nauka - Praktyka - Refleksje, 2015 r., nr 20, s. 239 – 240.

WNIOSKI

Według danych przedstawionych przez Komendę Główną Państwowej Straży Pożarnej jednostki ochrony przeciwpożarowej interweniują w około 500 tyś. zdarzeniach rocznie. Do zagrożeń zaś podstawowych należą: pożary, powodzie i zatopienia, katastrofy komunikacyjne i budowlane, wybuchy gazów, przypadki wycieków substancji i środków chemicznych. Można powiedzieć, że w tym zakresie efektywnie prowadzone są działania ratownicze w stosunku do zagrożeń. Stan ten świadczy o skuteczności sił i o właściwym stosowaniu środków Krajowego Systemu Ratowniczo-Gaśniczego. Biorąc pod uwagę działania prowadzone przez funkcjonariuszy należy stwierdzić, że potwierdzają one ich profesjonalizm. Wskazane jest dalsze tworzenie warunków do funkcjonowania Krajowego Systemu Ratowniczo-Gaśniczego, aby jego siły i środki mogły lepiej ze sobą współdziałać i współpracować z innymi służbami w ramach zorganizowanego systemu ratownictwa w Rzeczypospolitej Polskiej. Krajowy System Ratowniczo-Gaśniczy stanowi integralną część bezpieczeństwa wewnętrznego państwa, mającą na celu ratowanie życia, zdrowia, mienia lub środowiska, prognozowanie, rozpoznawanie i zwalczanie pożarów, klęsk żywiołowych lub innych miejscowych zagrożeń. Z konstrukcji systemu wynika, że realizowane podstawowe zadania ratownicze są niezmienne i dostosowane do specyfiki wszelkiego rodzaju zdarzenia, w tym o charakterze masowym. Powyższy system funkcjonuje w sposób ciągły, w stanie stałego czuwania i doraźnego reagowania polegającym na podejmowaniu działań ratowniczych. Działania te realizowane są własnymi siłami systemu oraz środkami powiatu i gmin. W sytuacji, gdyby siły i środki ratownicze okazałyby się niewystarczające wskazane będą modyfikacje i zmiana procedur organizacji działań ratowniczych. Zgodnie z ustawami Państwowa Straż Pożarna posiada odpowiednie struktury organizacyjne – struktura trójszczeblowa (Komendant Główny Państwowej Straży Pożarnej – jako centralny organ administracji rządowej w sprawach organizacji Krajowego Systemu Ratowniczo-Gaśniczego oraz ochrony przeciwpożarowej, komendanci wojewódzki i powiatowy). Współdziałanie poszczególnych organów i jednostek składają się na zorganizowaną całość, dającą możliwość realizacji nałożonych zadań. Wykonywaniu zadań służą określone środki i instrumenty działania. Współdziałanie wszystkich wymienionych instytucji przyczynia się do zmniejszania zagrożeń, ma zapewnić skuteczne rozpoznanie, służyć ochronie życia i zdrowia oraz mienia obywateli. W dalszym ciągu należy jednak rozwijać współpracę z innymi państwami i aktywniej uczestniczyć w pracach międzynaro-

dowych struktur i w ćwiczeniach organizowanych w kraju i za granicą, a także akcjach ratowniczych.

Każda organizacja, aby sprawnie działać, musi dostosowywać się do otaczającej rzeczywistości, na bieżąco obserwować zachodzące zmiany w otoczeniu i przystosowywać się do nich, celem zapewnienia realizacji stawianych przed nią celów

Analiza przedstawionych rozważań w niniejszej dysertacji związanej z funkcjonowaniem i organizacją formacji Państwowej Straży Pożarnej pozwala stwierdzić, iż jest ona systemem społeczno-technicznym. W skład takiego systemu wchodzą cztery podstawowe elementy, do których zaliczyć należy: ludzi, strukturę, zadania i technologie. Na organizację ponadto składają się podsystemy celów, struktury, psychospołeczny oraz techniczny.

Dla realizacji ustawowych i zakładanych celów dla których powołana jest Państwowa Straż Pożarna wszystkie wyżej wymienione elementy muszą być bez wątpienia ze sobą w logiczny sposób powiązane i uporządkowane. Podstawowym i najważniejszym zasobem omawianej instytucji jest czynnik ludzki posiadający stosowne kompetencje. To dzięki funkcjonariuszom/pracownikom organizacja realizujący stawiane przed nią cele i zadania. Odbywa się to z wykorzystaniem dostępnych technologii oraz środków technicznych, do których możemy zaliczyć maszyny, urządzenia czy sprzęt komputerowy. Natomiast zadaniem każdego kierującego daną organizacją czy jednostką organizacyjną jest zapewnienie prawidłowo zbudowanej struktury organizacyjnej, która powinna określać konkretne formy podziału zadań, kompetencji i odpowiedzialności.

W przypadku Państwowej Straży Pożarnej, gdzie mowa jest o organizacji zhierarchizowanej, w dysertacji poddano analizie właśnie taki rodzaj organizacji, co pozwala stwierdzić, że struktura tej instytucji ma charakter smukły o budowie hierarchicznej. Określone jest w niej podporządkowanie stanowisk znajdujących się niżej w hierarchii stanowiskom wyższego szczebla. Tym samym stwierdzić można, że ten typ organizacji wyróżnia się budową wieloszczeblową.

Kolejną istotną cechą charakteryzującą organizację zhierarchizowaną jest to, że wytyczne, polecenia i rozkazy przekazywane są od góry do dołu na każdym szczeblu podporządkowania, przy czym główną rolę ogrywają więzi służbowe, rozpiętość kierowania i linie podporządkowania.

W oparciu o literaturę przedmiotu, ale także osobiste obserwacje autora niniejszej dysertacji należy stwierdzić, że sprawne działanie organizacji uwarunkowane jest jej skutecznością. Dlatego też w każdym przypadku stwierdzenia nieprawidłowości

w funkcjonowaniu instytucji należy bezzwłocznie dokonać diagnozy zagrożonych obszarów działania organizacji i wprowadzić w życie programy naprawcze celem zwiększenia skuteczności jej działania.

Należy przy tym zwrócić szczególną uwagę na podatność informatyczną, czyli słabość danego systemu informatycznego wynikającą z błędów wewnętrznych lub błędów użytkownika. Poziom bezpieczeństwa jest jednym z aspektów użyteczności systemów informatycznych, które są gromadzone i eksploatowane przez Państwową Straż Pożarną.

Przydatność aplikacji jest tym większa im większy zapewnia poziom bezpieczeństwa. W XXI wieku istnieje wiele organizacji rozproszonych, biur wirtualnych ze strukturą sieciową, gdzie bezpieczeństwo danych i komunikacji jest sprawą najwyższej rangi. Informacja w organizacji stanowi strategiczny komponent, gromadzenie, przetwarzanie i udostępnianie, wszystko co wpływa na wzrost ilości danych komplikuje kwestie automatyzacji procesów informatycznych, które wymagają odpowiednich środków ochrony. Z perspektywy czasu określono, że jakość systemu informatycznego określa skalę efektu synergii, tym samym pozycję konkurencyjną instytucji.

Podejście procesowe obecne w systemach transakcyjnych, informatyczno-raportujących, systemach wspomagania decyzji oraz sztucznej inteligencji wymaga integracji danych i usług, gdzie platformą integracji są systemy zintegrowane.

Jednocześnie wydaje się, że zbyt duża rozpiętość i zasięg kierowania organizacją jaką jest Państwowa Straż Pożarna negatywnie wpływa na poprawne jej funkcjonowanie, co z kolei wpływa na procesy informacyjne i komunikację. Uwzględniając także stosowane rozwiązania komunikacyjne zasadnym wydaje się podjęcie działań zmierzających do usprawnienia obiegu informacji, co powinno przełożyć się na skuteczność działania w przypadku organizacji zhierarchizowanej.

Ochrona danych wymaga podejścia systemowego. Dotyczy to środowiska, w którym działa system. Różne środowiska będą obarczone lukami, które są konsekwencją błędów w projektowaniu systemu oraz niezapewnienia dostatecznych środków zabezpieczenia. Jednocześnie dynamika rozwoju systemów oraz zagrożeń powoduje konieczność wytwarzania elastycznych i podatnych na zmiany rozwiązań zabezpieczających, które pozwolą na modyfikację w krótkim czasie w przypadku zmiany środowiskowej. Zagrożenia stanowią działania ukierunkowane na składowe systemu informatycznego mogące powodować szkody. W celu zwiększenia bezpieczeństwa danych opisuje się zabezpieczenia normami i standardami bezpieczeństwa.

Każdy zasób jest wrażliwy na szereg potencjalnych zagrożeń, problemy które dany zasób może realnie napotkać należy spisać i ocenić pod kątem możliwości wystąpienia i konsekwencji jakie im towarzyszą. Lista powstaje w oparciu o wiedzę ekspercką kierowaną zdrowym rozsądkiem. Analiza podatności jest trudna i żmudna, ponieważ dla różnych zasobów zagrożenia powtarzają się ale wymagają kontekstowej analizy. Dlatego należy przyjąć poziom szczegółowości na jakim dokonuje się analizy. Wstępnie najlepiej jest zacząć od poziomu ogólnego, a w przypadku stwierdzenia konieczności przejść do bardziej szczegółowej analizy.

W pierwszej kolejności należy określić listę potencjalnych zagrożeń dla różnych zasobów:

- zalanie (w wyniku powodzi lub awarii sieci wodociągowej)
- pożar (wynikający z awarii lub podpalenia)
- atak grupy hackerskiej,
- kradzież danych przez osoby uprawnione i nieuprawnione
- fizyczne uszkodzenie nośników danych,
- awaria sprzętu towarzyszącego,
- brak zasilania,
- zagubienie / kradzież sprzętu zawierającego istotne dane,
- wyciek danych osobowych.

W ramach realizowanego przedsięwzięcia modernizacji SWD PSP należy dokonać zmiany architektury z rozproszonej na scentralizowaną, co usprawni procesy obsługi zdarzeń oraz umożliwi łatwiejszą integrację z zewnętrznymi systemami teleinformatycznymi, w tym w szczególności z systemem powiadamiania ratunkowego. Nowe SWD PSP powinno być także platformą współpracy z jednostkami Ochotniczych Straży Pożarnych, które powinny mieć nieodpłatny dostęp do modułu systemu. Jest to niezwykle istotna zmiana, której prawidłowe przeprowadzenie zdecydowanie poprawi komfort pracy dyżurnego stanowiska kierowania. W chwili dysponowania jednostek ochotniczych będzie on kierował się informacjami o tym, które jednostki OSP i w jakiej sile deklarują swój udział w akcji ratowniczej. Jednocześnie system umożliwi dostęp do informacji druhom ochotnikom, którzy w chwili otrzymania zgłoszenia będą wiedzieć, do jakiego zdarzenia się udają i ilu członków ich jednostki zadeklarowało gotowość bojową.

Nowy System SWD PSP powinien być także bardziej otwarty na integrację. Mowa tutaj w szczególności o integracji z systemami, które już teraz wspomagają druhów ochotników w potwierdzaniu ich gotowości bojowej. Po otrzymaniu zgłoszenia system automatycznie

powodowałby rozsyłanie wiadomości strażakom ochotnikom, którzy przynależą do danej jednostki. Dzięki zainstalowanej na telefonie komórkowym aplikacji ratownicy mieliby możliwość potwierdzenia lub negacji gotowości do udziału w akcji ratowniczej. Osoby, które zadeklarowałyby chęć udziału w akcji automatycznie wyświetlane zostaną na monitorze w jednostce OSP, co znacznie przyspiesza wyjazd do działań. Kierujący jednostką otrzymuje wówczas klarowną informację o liczbie druhów, którzy zadeklarowali udział w akcji ratowniczej, i widzi lokalizację tych osób. Podobną informacją dysponuje też dyżurny stanowiska kierowania.

Rozdział 4 KONCEPCJA BEZPIECZEŃSTWA SYSTEMU INFORMACYJNEGO W PAŃSTWOWEJ STRAŻY POŻARNEJ.

System wymiany informacji w Państwowej Straży Pożarnej, oprócz konieczności zapewnienia szybkiej, pewnej i sprawnej komunikacji na wielu płaszczyznach i poziomach w samej organizacji, stanowi również element Systemu Powiadamiania Ratunkowego w Polsce, będąc jego fundamentalną częścią, a tym samym podstawowym filarem systemu bezpieczeństwa wewnętrznego państwa.

Mając powyższe na uwadze koniecznym staje się zapewnianie jego ciągłego rozwoju, w tym zapewnienie bezpieczeństwa jego funkcjonowania, bezpieczeństwa zasobów IT, zwiększania efektywności, elastyczności, wydajności, a z drugiej strony obniżenia kosztów pracy.

Cyfryzacja jest dzisiaj kluczowym wyzwaniem dla administracji publicznej. Państwowa Straż Pożarna jest jedną z najmniej zdigitalizowanych instytucji w Polsce, ale jednocześnie jedną z najbardziej zaangażowanych w proces cyfryzacji. W najbliższych latach celem PSP powinno być mocne zaangażowania się i inwestycja w transformację cyfrową, co sprawi, że instytucja ta stanie się liderem w tej kwestii. Uruchomienie portalu danych statystycznych, rozwijanie usług dla obywateli i wprowadzenie nowoczesnych rozwiązań informatycznych to tylko niektóre z działań, które pomogą PSP w osiągnięciu tego celu.
Z jednej strony, wprowadzenie cyfryzacji pozwoli PSP na bardziej efektywne i skuteczne działanie, z drugiej strony, obywatele będą mieć łatwiejszy dostęp do informacji i będą w stanie szybciej załatwić swoje sprawy. Warto zauważyć, że cyfryzacja to nie tylko kwestia wygodniejszego dostępu do usług, ale także kwestia bezpieczeństwa i skuteczności działań PSP, dlatego proces ten w pierwszej kolejności powinien odnosić się do wspomagania każdego ze szczebli kierowania działaniami ratowniczymi. W ten sposób PSP będzie mieć bardziej efektywny dostęp do informacji i będzie w stanie szybciej reagować na pojawiające się zagrożenia. Wiedza, informacja i świadomość sytuacyjna dla każdego funkcjonariusza włączonego w proces kierowania działaniami ratowniczymi daje nieporównywalne możliwości w zakresie skutecznego zarządzania zasobami m.in. ludźmi i sprzętem, w tym pojazdami. Informacja z czym mamy do czynienia (jakim rodzajem zdarzenia, problemem) zestawiona z wiedzą osób ekspertów, którzy mogą zostać włączeni do procesu decyzyjnego przy użyciu narzędzi, w tym usług cyfrowych, jest remedium, dzięki któremu

w znacznie krótszym czasie jesteśmy w stanie przekazać żądany scenariusz w zakresie np. sposobu przeciwdziałania zagrożeniu, metod walki z zagrożeniem. Usługi cyfrowe powodują, że eksperci z danej dziedziny nie muszą znajdować się na miejscu zdarzenia, aby realizować pełne wsparcie służb ratowniczych.

W kolejnych etapach należy położyć nacisk na rozwijane kolejnych usług, tak aby obywatele mogli szybko i bezpiecznie załatwić swoje sprawy. Będzie to możliwe dzięki wprowadzeniu nowoczesnych rozwiązań informatycznych, takich jak elektroniczne formularze, platformy e-learningowe czy systemy do zarządzania zasobami.

W ramach projektowanej strategii należy zwrócić uwagę na proces modernizacji całej organizacji z wykorzystaniem technologii cyfrowych. Głównym celem tej strategii powinno stać się podniesienie sprawności państwa w zakresie zapobiegania zagrożeniom wewnętrznym oraz poprawa jakości relacji administracji z obywatelami i innymi interesariuszami.

Cyfryzacja procesów wewnątrz organizacji PSP powinna obejmować między innymi:

- zwiększenie jakości oraz zakresu komunikacji między obywatelami a państwem, dzięki czemu procesy związane z PSP będą bardziej przejrzyste i łatwiej dostępne dla obywateli.
- wzmocnienie dojrzałości organizacyjnej PSP oraz usprawnienie zaplecza elektronicznej administracji (back office) poprzez wykorzystanie nowoczesnych rozwiązań technologicznych.
- podniesienie poziomu kompetencji cyfrowych pracowników PSP poprzez szkolenia oraz stałe podnoszenie ich kwalifikacji.

Cyfryzacja procesów wewnątrz PSP pozwoli również na automatyzację wielu czynności, co przełoży się na oszczędność czasu i zasobów. Dzięki temu, pracownicy PSP będą mogli skoncentrować się na swoich głównych zadaniach, takich jak ochrona ludzi i mienia przed pożarami oraz innymi zagrożeniami. Warto również wspomnieć, że cyfryzacja procesów wewnątrz PSP pozwoli na lepsze zarządzanie danymi, co jest szczególnie ważne w przypadku instytucji odpowiedzialnej za bezpieczeństwo publiczne. Dzięki temu, PSP będzie mogła szybciej reagować na zagrożenia oraz skuteczniej koordynować swoje działania.

Chcąc sprostać temu wyzwaniu niezbędnym stało się opracowanie zestawu technologii pozwalających na bardziej efektywną wyminę informacji i komunikacji ICT (Information and Communication Technology). ICT to pojęcie obejmujące szeroki zakres rozwiązań i narzędzi, które służą do przetwarzania, przesyłania, przechowywania

i dostarczania informacji. Obejmuje ono sprzęt, oprogramowanie, systemy teleinformatyczne i usługi, które wykorzystuje się w celu zwiększenia efektywności, w tym efektywności komunikacji oraz zarządzania informacjami. ICT zawiera zarówno komponenty związane z przetwarzaniem danych (np. serwery, komputery, bazy danych), jak i te związane z ich przesyłaniem i dostępnością (np. sieci komputerowe, telefony komórkowe, aplikacje mobilne). ICT ma kluczowe znaczenie dla rozwoju, pozwala na lepsze zarządzanie informacją, usprawnienie wszelkich procesów i zwiększenie efektywności działań organizacji.

Prawidłowe i optymalne funkcjonowanie krajowego systemu ratowniczo gaśniczego opiera się o dostęp do wiedzy stanowisk kierowania PSP. W związku z powyższym, koniecznym staje się stworzenie odpornego na awarie, heterogenicznego systemu, w tym teleinformatycznego, dzięki któremu dyżurny stanowiska będzie mógł realizować skutecznie zadania w ramach obowiązującego prawa. System co do zasady musi być odporny na szerokorozumiane zagrożenia w zakresie cyberbezpieczeństwa, dawać możliwość dostosowywania go do własnych potrzeb, ze szczególnym uwzględnieniem spójnego jednolitego systemu komunikacji. Kluczem do sukcesu nie są tu tylko urządzenia, ale spójnie zaprojektowany system informatyczny umożliwiający komunikację praktycznie na każdym poziomie od przesyłanych danych tekstowych, poprzez rozmowy w ramach technologii VOIP, czy wideokonferencję. Formuła tego systemu powinna spełniać podstawowe wymagania w zakresie bezpieczeństwa informacji jak i dostępu oraz autoryzacji do systemu, co zapewni zbudowane i uruchomione rozwiązanie w ramach usług „cloud computing" w postaci hybrydowej. System taki z założenia musi integrować się (być kompatybilny) z rozwiązaniami już istniejącymi w polskim systemie teleinformatycznym. Organizacja, modernizacja oraz utrzymywanie takiego systemu powinno odbywać się centralnie, w tym przypadku przez organ jakim jest Komendant Główny Państwowej Straży Pożarnej.

Podjęte w niniejszym rozdziale dociekania mają na celu zobrazowanie przedstawionego w dysertacji celu utylitarnego, który został zdefiniowany jako opracowanie *koncepcji bezpieczeństwa systemu obiegu informacji w organizacji publicznej jaką jest Państwowa Straż Pożarna,* w odniesieniu do rozwiązania szczegółowego problemu badawczego wyrażonego w pytaniu: *Jaka powinna być koncepcja systemu obiegu informacji w Państwowej Straży Pożarnej, aby poprawić skuteczność jego funkcjonowania?*
Odbyło się to z uwzględnieniem oceny prawdziwości stawianej hipotezy, która stanowi przypuszczenie, że *należy poprawić skuteczność obiegu informacji oraz zwiększyć efektyw-*

ność zabezpieczeń informacji wewnątrz organizacji publicznej jaką jest Państwowa Straż Pożarna. Aby tego dokonać należałoby ujednolicić systemy teleinformatyczne na wszystkich poziomach organizacyjnych tej formacji oraz wprowadzić zmiany pod kątem organizacyjnym, technicznym i funkcjonalnym w zasadach użytkowania, funkcjonowania i organizacji systemu informacyjnego. Istotne jest wdrożenie i utrzymanie właściwego systemu zarządzania bezpieczeństwem informacji, który będzie umożliwiał ochronę wszystkich przetwarzanych informacji, jak również zapewniał ciągłość realizowanych procesów i zadań. Aby osiągnąć jak najwyższy stopień bezpieczeństwa informacji, należy w odpowiedni sposób przygotować zasoby organizacji, a następnie odpowiednio i odpowiedzialnie nimi zarządzać. Zakłada się, że niezbędne dla ochrony informacji w instytucji jest właściwie ułożenie i konsekwentne egzekwowanie polityki bezpieczeństwa informacji, co jest elementem decydującym o jej skuteczności, a systematyczny wielopłaszczyznowy nadzór zwiększa bezpieczeństwo informacji będących w obiegu.

W celu rozwiązania problemu badawczego oraz weryfikacji sformułowanej hipotezy, przyjęto następujące metody badawcze:

1. teoretyczne:

a) analizę – stosowaną głównie w badaniu literatury przedmiotu,

b) syntezę – wykorzystywaną głównie podczas łączenia efektów analizy w syntetyczną całość,

2. empiryczne:

a) sondaż diagnostyczny badania opinii techniką ankiety z wykorzystaniem narzędzia w postaci arkusza ankiety – pozwalający na poznanie opinii respondentów na temat systemu informacyjnego w Państwowej Straży Pożarnej;

b) metodę obserwacji techniką obserwacji z wykorzystaniem narzędzia w postaci arkusza obserwacji – celem której będzie zebranie wszelkich spostrzeżeń związanych z systemem informacyjnym w Państwowej Straży Pożarnej

Oczywiście w celu zbadania tematu konieczne było zastosowanie innych metod teoretycznych w postaci:

- abstrahowania – w celu wyodrębnienia lub pominięcia pewnych elementów związanych z systemem informacyjnym, które z pewnych przyczyn uznano za istotne, mające wpływ na analizowane zagadnienie oraz te, które dla tej analizy nie mają większego znaczenia,
- uogólnienia – polegające na łączeniu określonych przedmiotów analizy w oparciu o ich podobieństwa,

- porównania – zestawienie cech wspólnych i różnicujących przedmiot badań,
- wnioskowania – wypracowanie spostrzeżeń będących przedmiotem analizy bezpieczeństwa systemu informacyjnego.

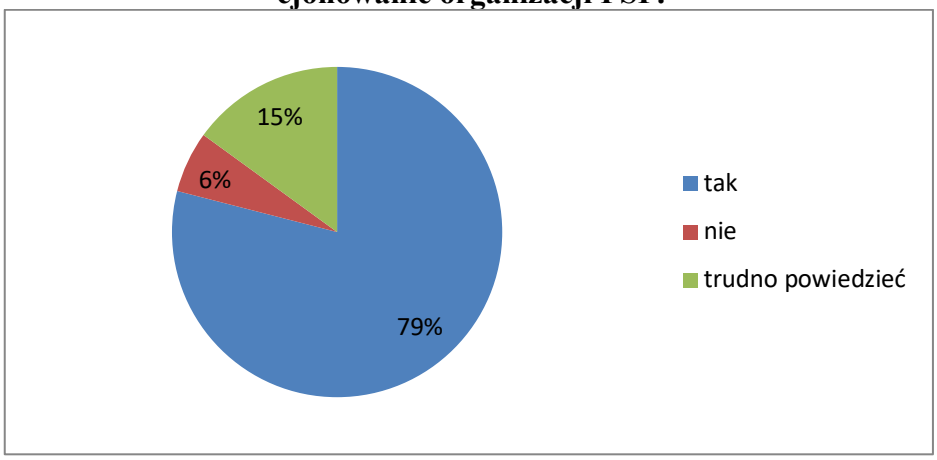
4.1 ANALIZA WYNIKÓW BADAŃ.

W ramach przeprowadzonych badań empirycznych poproszono ankietowanych o udzielenie odpowiedzi na pierwsze pytanie (zał. 1): *1. Czy uważa Pani/Pan, że system informacyjny (system wymiany informacji) ma strategiczny wpływ na funkcjonowanie jednostki macierzystej i całej organizacji PSP?*

Uczestnikom zaproponowano trzy warianty odpowiedzi jednokrotnego wyboru, a mianowicie: tak, nie i trudno powiedzieć. W wyniku czego uzyskano 1897 wskazań, na co składało się 352 odpowiedzi I grupy – pracowników KW PSP i 1545 odpowiedzi II grupy – pracowników KM/KP PSP. Ogólny rozkład odpowiedzi został zawarty na poniższym wykresie 4-1. Analizując wyniki, można zauważyć, iż respondenci zdecydowanie opowiedzieli się za wariantem odpowiedzi, iż system informacyjny ma strategiczny wpływ na organizację PSP i jej funkcjonowanie. Dowodem tego jest procentowy udział odpowiedzi na tak wśród respondentów, kształtujący się na poziomie 79 %, czyli 1494 wskazania. Część respondentów, która wskazała na brak takiej zależności stanowiła tylko 6 % odpowiadających, co stanowiło 112 wskazań na nie. Natomiast osoby, które nie miały określonego zdania w tym temacie stanowiły 15 %, na co złożyło się 291 wskazań wariantu odpowiedzi – trudno powiedzieć.

Szczegółowy rozkład odpowiedzi respondentów został ukazany w tabeli 4-1.

Wykres 4-1
Procentowy rozkład odpowiedzi dotyczący wpływu systemu informacyjnego na funkcjonowanie organizacji PSP.



Źródło: Opracowanie własne.

Badani należący do pierwszej grupy najczęściej wskazywali na wariant odpowiedzi tak – 86 % (302 wskazania), na drugim miejscu ukształtowała się odpowiedź trudno powiedzieć – 10 % (35 wskazań) i dalej odpowiedź nie – 4 % (15 wskazań).

Podobny rozkład wyników ukształtował się w drugiej grupie respondentów. Ankietowani najczęściej dokonywali wyboru odpowiedzi tak – 77 % (1191 wskazań), kolejno padała odpowiedź trudno powiedzieć – 17 % (256 wskazania) i na trzecim miejscu nie – 6 % (98 wskazań).

Szczegółowy rozkład odpowiedzi dotyczący wpływu systemu informacyjnego na organizację i jej funkcjonowanie zaprezentowano w tabeli 4-1.

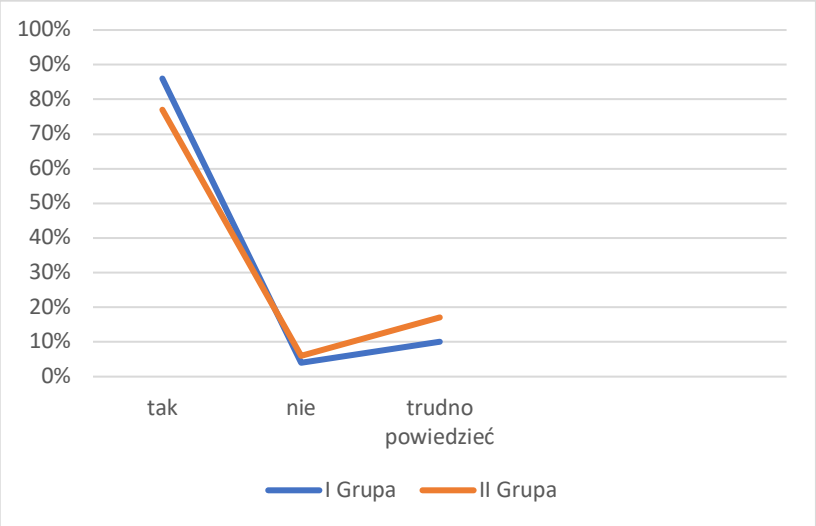
Tabela 4-1
Procentowy rozkład odpowiedzi dotyczący wpływu systemu informacyjnego na funkcjonowanie organizacji PSP.

Odpowiedzi	I Grupa PRACOWNICY KW		II Grupa PRACOWNICY KM/KP		Ogółem	
	Struktura liczbowa	Struktura procentowa (%)	Struktura liczbowa	Struktura procentowa (%)	Struktura liczbowa	Struktura procentowa (%)
tak	302	86	1191	77	1493	79
nie	15	4	98	6	113	6
trudno powiedzieć	35	10	256	17	291	15
Ogółem	352	100	1545	100	1897	100

Źródło: Opracowanie własne.

W celu dokładniejszego zobrazowania uzyskanych rozkładów udzielonych odpowiedzi z obu grup, wyniki zaprezentowano na wykresie 4-2.

Wykres 4-2
Procentowy rozkład odpowiedzi w obu grupach badawczych dotyczący wpływu systemu informacyjnego na organizację PSP.



Zaprezentowany, powyższy wykres wskazuje na niewielkie rozbieżności, które wynikają z udzielonych odpowiedzi przez uczestników obydwu grup. W celu zbadania tejże istotności wykonano test współczynnika korelacji liniowej r- Pearsona.

Tabela 4-2
Rozkład odpowiedzi dotyczący wpływu systemu informacyjnego na funkcjonowanie organizacji PSP

Odpowiedzi	I Grupa KW	II Grupa KM/KP	Ogółem		
	x_i	y_i	x_i^2	y_i^2	$x_i * y_i$
tak	302	1191	91204	1418481	359682
nie	15	98	225	9604	1470
trudno powie-dzieć	35	256	1225	65536	8960
Ogółem	$\sum_{i=3}^{n} x_i$= 352	$\sum_{i=3}^{n} y_i$= 1545	$\sum_{i=3}^{n} x_i^2$ = 92654	$\sum_{i=3}^{n} y_i^2$ = 1493621	$\sum_{i=3}^{n} x_i * y_i$ = 370112
$\bar{x} = \frac{1}{n}\sum_{i=n}^{n} x_i = \frac{1}{3} * 352 \approx 117$ $x^2 \approx 13\,689$ | $\bar{y} = \frac{1}{n}\sum_{i=n}^{n} y_i = \frac{1}{3} * 1545 \approx 509$ $y^2 \approx 259\,081$					

Źródło: Opracowanie własne.

$$r = \frac{\frac{1}{n}\sum_{i=n}^{n} x_i y_i - xy}{\sqrt{(\frac{1}{n}\sum_{i=n}^{n} x_i^2 - x^2)(\frac{1}{n}\sum_{i=n}^{n} y_i^2 - y^2)}} = \frac{\frac{1}{3} * 370112 - 59044}{\sqrt{(\frac{1}{3} * 92654 - 13689)(\frac{1}{3} * 1493621 - 259081)}} \approx 0{,}99$$

Po przeprowadzeniu testu współczynnika korelacji liniowej r- Pearsona, otrzymano wynik r ≈ 0,99, co świadczy o tym, iż wzrost wartości w odpowiedziach u jednej z grup powoduje wzrost wartości odpowiedzi w grupie drugiej.

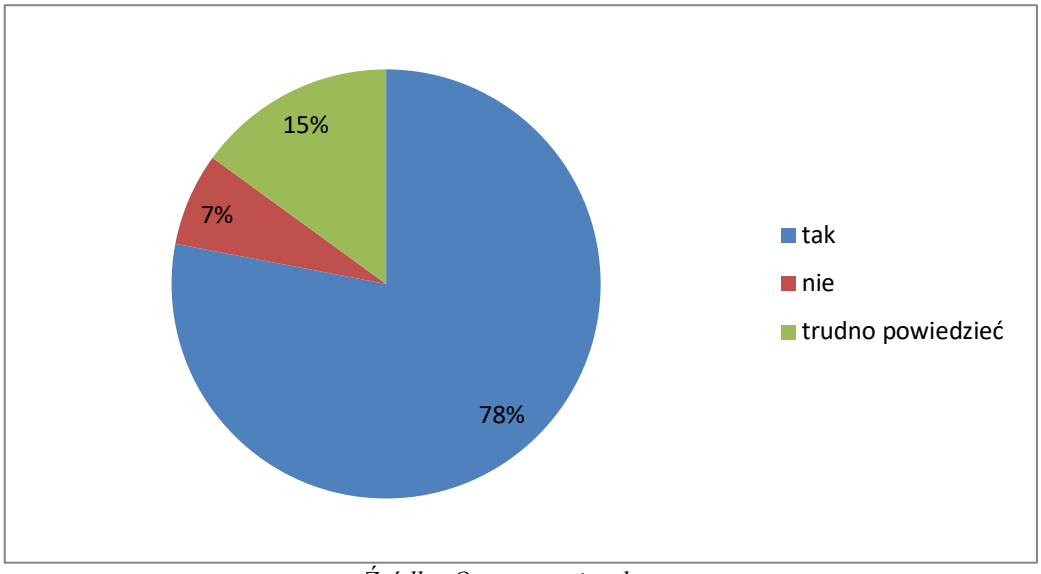
W ramach przeprowadzonych badań empirycznych poproszono respondentów o udzielenie odpowiedzi na kolejne pytanie nr 2 (zał. nr 1) *2. Czy uważa Pani/Pan, że zapewnienie bezpieczeństwa systemu informacyjnego (identyfikacja zagrożeń i możliwych usprawnień) jest podstawowym zadaniem instytucji publicznej w dzisiejszych czasach?*

Respondenci mieli do wyboru takie same warianty odpowiedzi jak w pierwszym pytaniu, czyli: tak, nie i trudno powiedzieć. Ogólny rozkład odpowiedzi został zilustrowany na wykresie 4-3. Wynika z niego, iż najwięcej wskazań otrzymała pierwsza zaproponowana możliwość tak, mówiąca o istocie bezpieczeństwa systemu informacyjnego dla dzisiejszych instytucji publicznych. Dowodem tego jest procentowy udział kształtujący się na poziomie 78 %, co stanowi 1476 wskazań respondentów obu grup. Na odpowiedź przeczącą zdecydowała się grupa 7 % ankietowanych, co stanowiło tylko 129 wszystkich

wskazań. Natomiast osoby, które nie miały określonego zdania w tym temacie stanowiły 15 %, na co złożyło się 292 wskazań wariantu odpowiedzi – trudno powiedzieć.

Szczegółowy rozkład odpowiedzi został ukazany w tabeli 4-3.

Wykres 4-3
Procentowy rozkład odpowiedzi dotyczący istoty bezpieczeństwa systemu informacyjnego dla dzisiejszych instytucji publicznych.



Źródło: Opracowanie własne.

Respondenci należący do I grupy najczęściej wskazywali na odpowiedź twierdzącą, że zapewnienie bezpieczeństwa systemu informacyjnego jest podstawowym zadaniem instytucji publicznej w dzisiejszych czasach – odpowiedź ta uzyskała aż 83 %, co stanowiło 292 wskazania. Na drugim miejscu uplasował się wariant odpowiedzi trudno powiedzieć, gdzie wskazania takiego dokonały 43 osoby, co dało wynik 12 % respondentów. Natomiast na wariant odpowiedzi nie, odpowiedziało tylko 5 % ankietowanych z liczbą 17 wskazań.

Podobnie ukształtował się układ procentowy odpowiedzi udzielonych przez respondentów II grupy. Najwięcej odpowiedzi otrzymała odpowiedź pierwsza tak, o czym świadczy 77 %, czyli 1185 wskazań. Następnie 16 % uzyskał wariant odpowiedzi trudno powiedzieć z liczbą 248 wskazań. Wariant z odpowiedzią nie uplasował się na trzecim miejscu z wynikiem zaledwie 7 %, na co złożyły się 112 wskazań.

Szczegółowy rozkład danych odpowiedzi został ukazany w tabeli 4-3.

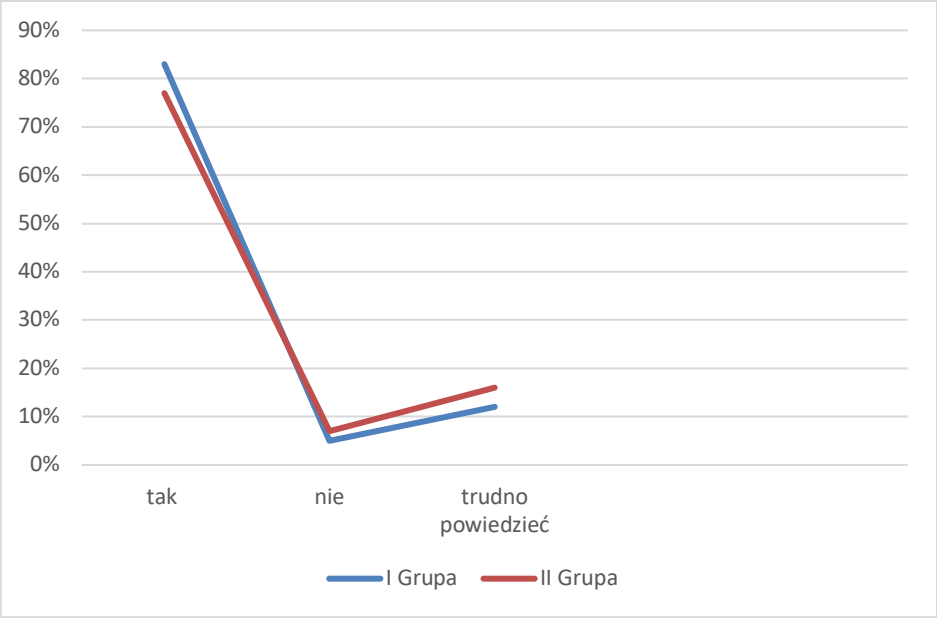
Tabela 4-3
Procentowy rozkład odpowiedzi dotyczący istoty zapewnienia bezpieczeństwa systemu informacyjnego jako podstawowego zadania dzisiejszej instytucji publicznej.

Odpowiedzi	I Grupa PRACOWNICY KW		II Grupa PRACOWNICY KM/KP		Ogółem	
	Struktura liczbowa	Struktura procentowa (%)	Struktura liczbowa	Struktura procentowa (%)	Struktura liczbowa	Struktura procentowa (%)
tak	292	83	1185	77	1 477	78
nie	17	5	112	7	129	7
trudno powiedzieć	43	12	248	16	291	15
Ogółem	352	100	1545	100	1897	100

Źródło: Opracowanie własne.

W celu dokładniejszego zobrazowania uzyskanych rozkładów udzielonych odpowiedzi z obu grup, wyniki zaprezentowano na wykresie 4-4.

Wykres 4-4
Procentowy rozkład odpowiedzi w obu grupach badawczych dotyczący istoty zapewnienie bezpieczeństwa systemu informacyjnego jako podstawowego zadania dzisiejszej instytucji publicznej.



Zaprezentowany, powyższy wykres wskazuje na niewielkie rozbieżności, które wynikają z udzielonych przez wszystkich ankietowanych odpowiedzi. W celu zbadania tejże istotności wykonano test współczynnika korelacji liniowej r- Pearsona.

Tabela 4-4
Rozkład odpowiedzi dotyczący istoty zapewnienie bezpieczeństwa systemu informacyjnego jako podstawowego zadania dzisiejszej instytucji publicznej

Odpowiedzi	I Grupa KW	II Grupa KM/KP	Ogółem		
	x_i	y_i	x_i^2	y_i^2	$x_i * y_i$
tak	292	1185	85264	1404225	346020
nie	17	112	289	12544	1904
trudno powiedzieć	43	248	1849	61504	10664
Ogółem	$\sum_{i=3}^{n} x_i =$ 352	$\sum_{i=3}^{n} y_i =$ 1545	$\sum_{i=3}^{n} x_i^2 =$ 87402	$\sum_{i=3}^{n} y_i^2 =$ 1478273	$\sum_{i=3}^{n} x_i * y_i =$ 358588
$\bar{x} = \frac{1}{n}\sum_{i=n}^{n} x_i = \frac{1}{3} * 352 \approx 117$ $x^2 \approx 13689$ | $\bar{y} = \frac{1}{n}\sum_{i=n}^{n} y_i = \frac{1}{3} * 1545 \approx 509$ $y^2 \approx 259\,081$					

Źródło: Opracowanie własne.

$$r = \frac{\frac{1}{n}\sum_{i=n}^{n} x_i y_i - xy}{\sqrt{(\frac{1}{n}\sum_{i=n}^{n} x_i^2 - x^2)(\frac{1}{n}\sum_{i=n}^{n} y_i^2 - y^2)}} = \frac{\frac{1}{3} * 358588 - 59044}{\sqrt{(\frac{1}{3} * 87402 - 13689)(\frac{1}{3} * 1478273 - 259081)}} \approx 0{,}99$$

Podobnie jak w pytaniu pierwszym i w tym przypadku po przeprowadzeniu testu współczynnika korelacji liniowej r- Pearsona, otrzymano wynik r ≈ 0,99, co świadczy, że pomiędzy poszczególnymi grupami występuje bardzo silna zależność i mówimy o korelacji dodatniej. Oznacza to, iż wzrost wartości odpowiedzi jednej z grup wpływa na wzrost wartości odpowiedzi drugiej z grup.

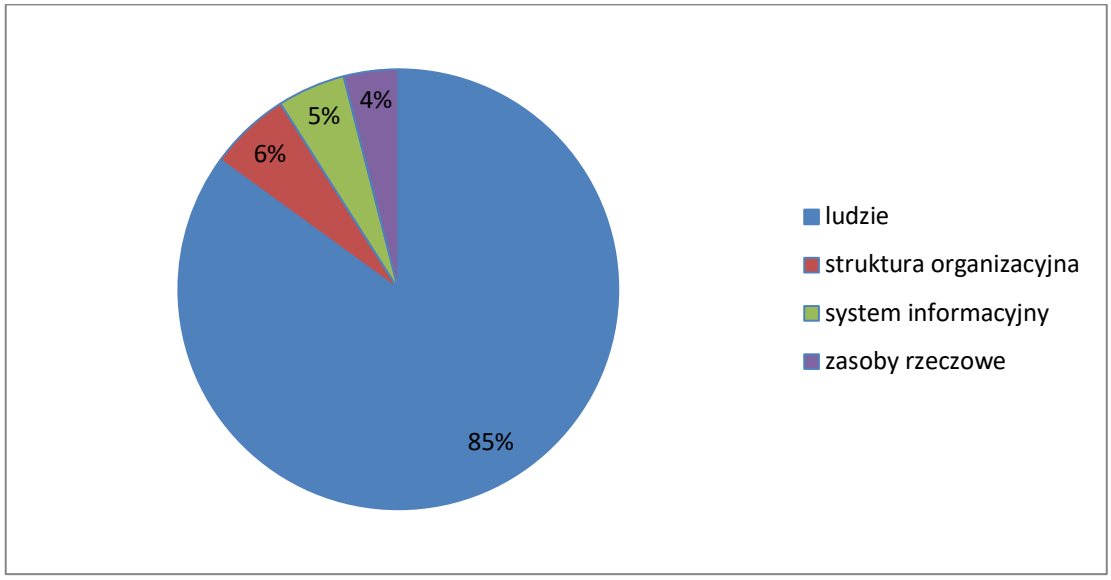
W ramach przeprowadzonych badań empirycznych poproszono respondentów o udzielenie odpowiedzi na pytanie trzecie (zał. 1): *3. Które z wymienionych poniżej podstawowych zasobów ma Pani/Pana zdaniem największy wpływ na skuteczne funkcjonowanie organizacji?*

Badanym zaproponowano cztery warianty odpowiedzi, jednokrotnego wyboru, w wyniku czego uzyskano 1897 wskazań. Ogólny rozkład odpowiedzi został zaprezentowany na wykresie 4-5, z którego wynika, iż najwięcej opiniodawców odpowiedziało się za wariantem, iż to ludzie są podstawowym zasobem organizacji, o czym świadczy 85 % uzyskanych odpowiedzi, na co złożyło się 1620 wskazań. Zdecydowanie mniej głosów respondentów uzyskały dwa pozostałe warianty odpowiedzi, a mianowicie: struktura organizacyjna – 6 % (119 wskazań), system informacyjny – 5 % próby badawczej (112 wska-

zań). Natomiast odpowiedź o zasobach rzeczowych wybrało tylko 4 %, co stanowiło 46 wskazań.

Szczegółowy rozkład został ujęty w tabeli 4-5.

Wykres 4-5
Procentowy rozkład odpowiedzi dotyczący zasobów mających największy wpływ na skuteczne funkcjonowanie organizacji.



Źródło: Opracowanie własne.

Respondenci należący do I grupy najczęściej wskazywali na odpowiedź, że to zasoby ludzkie są najistotniejsze w organizacji – odpowiedź ta uzyskała 87 %, co stanowiło 306 wskazania. Na drugim miejscu uplasował się wariant odpowiedzi, że to system informacyjny, gdzie wskazania takiego dokonało 24 respondentów – 7 %. Trzecim wariantem została odpowiedź o strukturze organizacyjnej, na którą zdecydowało się 17 ankietowanych - 5 %. Za najmniej istotny czynnik ankietowali uznali zasoby rzeczowe, tylko 5 wskazania, co daje 1 % całości odpowiedzi.

W II grupie ankietowanych także zdecydowana większość respondentów wybrała wariant odpowiedzi o zasobach ludzkich jako najistotniejszych w organizacji, 1314 wskazań – 85 %. Nieco inaczej wybory respondentów ukształtowały się w kolejnych odpowiedziach, gdzie wariant odpowiedzi o ważności struktury organizacyjnej wybrało 102 respondentów – 7 %, Natomiast trzecim wariantem w tej grupie została odpowiedź o systemie informacyjnym, na którą zdecydowało się 88 ankietowanych - 6 %. Podobnie jak w pierwszej grupie najrzadziej wybieraną odpowiedzią wśród ankietowanych dotyczą-

cą tego pytania była odpowiedź o zasobach rzeczowych, którą wybrało tylko 41 osób – 2 %.

Szczegółowy rozkład danych odpowiedzi został ukazany w tabeli 4-5.

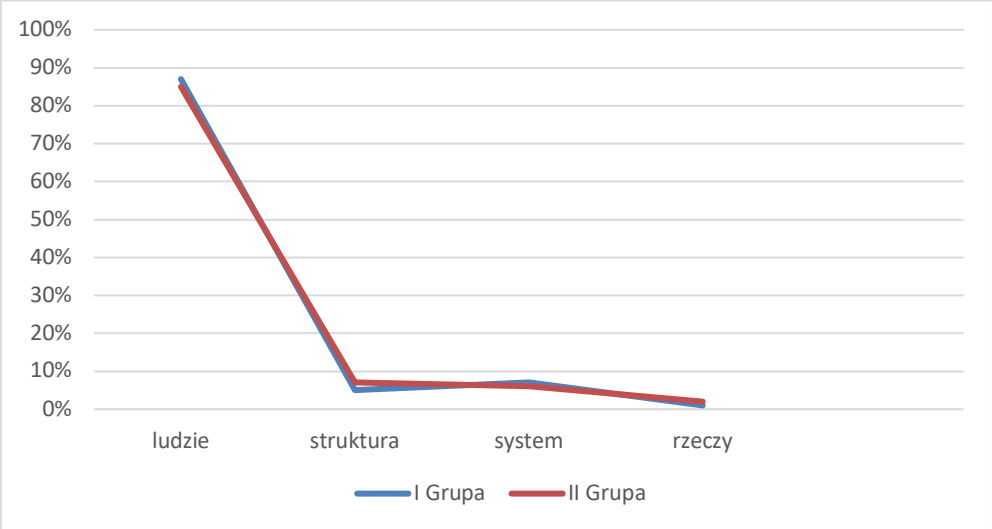
Tabela 4-5
Procentowy rozkład odpowiedzi dotyczący najistotniejszych zasobów organizacji.

Odpowiedzi	I Grupa PRACOWNICY KW		II Grupa PRACOWNICY KM/KP		Ogółem	
	Struktura liczbowa	Struktura procentowa (%)	Struktura liczbowa	Struktura procentowa (%)	Struktura liczbowa	Struktura procentowa (%)
ludzie	306	87	1314	85	1620	85
struktura organizacyjna	17	5	102	7	119	7
system informacyjny	24	7	88	6	112	6
zasoby rzeczowe	5	1	41	2	7	2
Ogółem	352	100	1545	100	1897	100

Źródło: Opracowanie własne.

W celu dokładniejszego zobrazowania uzyskanych rozkładów udzielonych odpowiedzi z obu grup, wyniki zaprezentowano na wykresie 4-6.

Wykres 4-6
Procentowy rozkład odpowiedzi w obu grupach badawczych dotyczący zasobów mających największy wpływ na skuteczne funkcjonowanie organizacji.



Zaprezentowany, powyższy wykres wskazuje na minimalne rozbieżności, które wynikają z udzielonych przez wszystkich ankietowanych odpowiedzi. W celu zbadania tejże istotności wykonano test współczynnika korelacji liniowej r- Pearsona.

Tabela 4-6

Rozkład odpowiedzi dotyczący najistotniejszych zasobów organizacji.

Odpowiedzi	I Grupa KW	II Grupa KM/KP	Ogółem		
	x_i	y_i	x_i^2	y_i^2	$x_i * y_i$
ludzie	306	1314	93636	1726596	402084
struktura organizacyjna	17	102	289	10404	1734
system informacyjny	24	88	576	7744	2112
zasoby rzeczowe	5	41	25	1681	205
Ogółem	$\sum_{i=3}^{n} x_i =$ 352	$\sum_{i=3}^{n} y_i =$ 1545	$\sum_{i=3}^{n} x_i^2 =$ 94526	$\sum_{i=3}^{n} y_i^2 =$ 1746425	$\sum_{i=3}^{n} x_i * y_i =$ 406135
$\bar{x} = \frac{1}{n}\sum_{i=n}^{n} x_i = \frac{1}{4} * 352 \approx 88$ $x^2 \approx 7\,744$ | $\bar{y} = \frac{1}{n}\sum_{i=n}^{n} y_i = \frac{1}{4} * 1545 \approx 386$ $y^2 \approx 148\,996$					

Źródło: Opracowanie własne.

$$r = \frac{\frac{1}{n}\sum_{i=n}^{n} x_i y_i - xy}{\sqrt{(\frac{1}{n}\sum_{i=n}^{n} x_i^2 - x^2)(\frac{1}{n}\sum_{i=n}^{n} y_i^2 - y^2)}} = \frac{\frac{1}{4} * 406135 - 33\,968}{\sqrt{(\frac{1}{4} * 94526 - 7\,744)(\frac{1}{4} * 1746425 - 148\,996)}} \approx 0{,}99$$

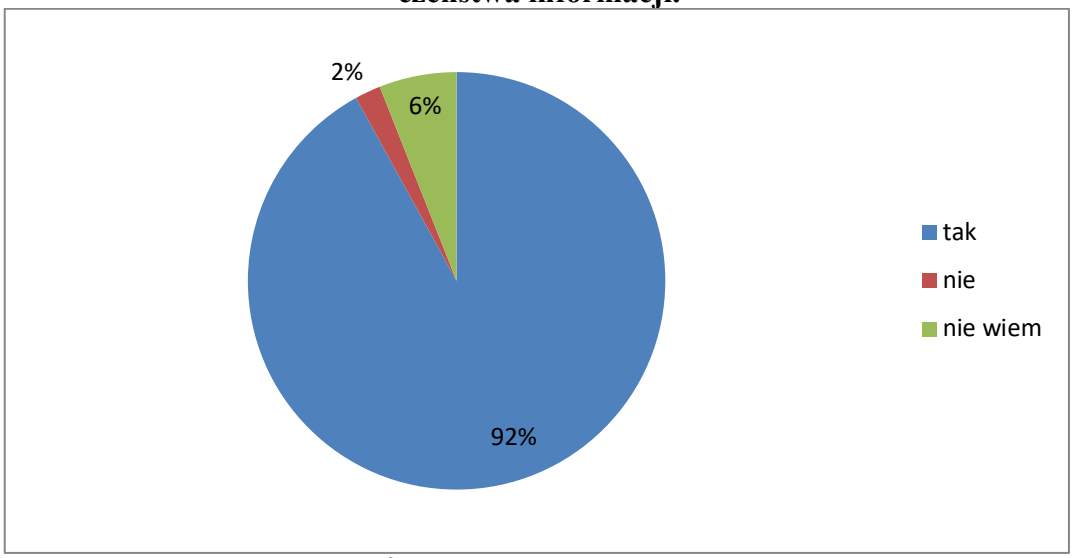
Obliczony współczynnik wynosi w przybliżeniu r = 0,99 i należy stwierdzić, iż jest to korelacja dodatnia o bardzo wysokim charakterze. Świadczy to o występującej dość silnej zależności pomiędzy przynależnością do grupy, a wskazywaniem danej odpowiedzi oraz oznacza to, iż wzrost wartości odpowiedzi jednej z grup wpływa na wzrost wartości odpowiedzi drugiej z grup.

W ramach przeprowadzonych badań empirycznych poproszono respondentów o udzielenie odpowiedzi na następne czwarte z kolei pytanie (zał. nr 1) 4. *Czy w Pani/Pana jednostce wprowadzone są procedury, regulaminy i instrukcje – polityka bezpieczeństwa informacji?* Respondenci mieli do wyboru następujące warianty odpowiedzi: tak, nie i nie wiem.

Ogólny rozkład odpowiedzi został zilustrowany na wykresie 4-7. Wynika z niego, iż najwięcej wskazań otrzymała pierwsza zaproponowana możliwość tak, potwierdzająca fakt wdrożenia takich procedur i instrukcji w PSP. Dowodem tego jest procentowy udział kształtujący się na poziomie aż 92 % odpowiedzi, co stanowi 1740 wskazań respondentów obu grup. Na odpowiedź przeczącą zdecydowała się tylko grupa 2 % ankietowanych, co stanowiło 39 ze wszystkich wskazań. Natomiast osoby, które nie miały wiedzy w tym zakresie stanowiły 6 %, na co złożyło się 118 wskazań wariantu odpowiedzi – nie wiem.

Szczegółowy rozkład odpowiedzi został ukazany w tabeli 4-7.

Wykres 4-7
Procentowy rozkład odpowiedzi dotyczący wprowadzenia procedur – polityki bezpieczeństwa informacji.



Źródło: Opracowanie własne.

Respondenci należący do I grupy najczęściej wskazywali na odpowiedź potwierdzającą wprowadzenie procedur – polityki bezpieczeństwa informacji w PSP, gdyż odpowiedź ta uzyskała aż 94 %, co stanowiło 332 wskazania. Następnie wariant odpowiedzi nie wiem, wskazało 14 osób, co dało wynik 4 % respondentów. Natomiast na wariant odpowiedzi nie, odpowiedziało zaledwie 2 % ankietowanych z liczbą 6 wskazań.

Bardzo podobnie kształtował się układ odpowiedzi udzielonych przez respondentów II grupy. Najwięcej odpowiedzi otrzymała odpowiedź tak, o czym świadczy 91 %, czyli 1408 wskazań. Następnie 7 % uzyskał wariant odpowiedzi nie wiem z liczbą 104 wskazań. Wariant z odpowiedzią nie uplasował się na ostatnim miejscu z wynikiem 2 %, na co złożyły się 33 wskazania.

Szczegółowy rozkład danych odpowiedzi został ukazany w tabeli 4-7.

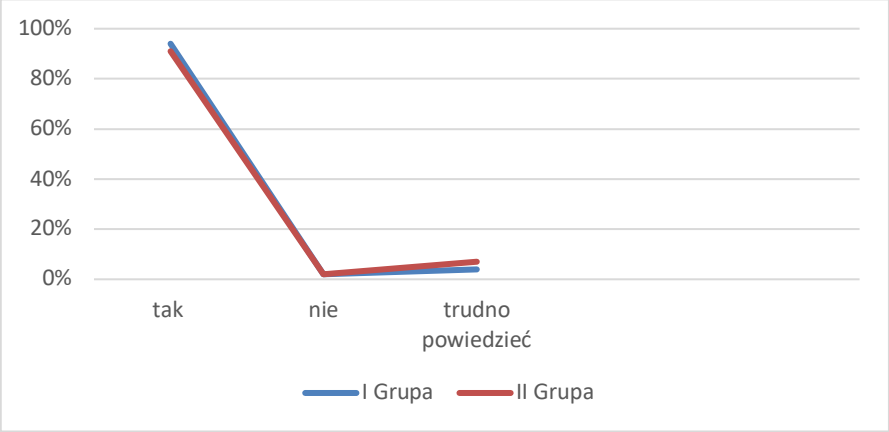
Tabela 4-7
Procentowy rozkład odpowiedzi dotyczący wprowadzenia w PSP procedur – polityki bezpieczeństwa informacji.

Odpowiedzi	I Grupa PRACOWNICY KW		II Grupa PRACOWNICY KM/KP		Ogółem	
	Struktura liczbowa	Struktura procentowa (%)	Struktura liczbowa	Struktura procentowa (%)	Struktura liczbowa	Struktura procentowa (%)
tak	332	94	1408	91	1 740	92
nie	14	4	104	7	118	2
nie wiem	6	2	33	2	39	6
Ogółem	352	100	1545	100	1897	100

Źródło: Opracowanie własne.

W celu dokładniejszego zobrazowania uzyskanych rozkładów udzielonych odpowiedzi z obu grup, wyniki zaprezentowano na wykresie 4-8.

Wykres 4-8
Procentowy rozkład odpowiedzi w obu grupach badawczych dotyczący wprowadzenia w PSP procedur – polityki bezpieczeństwa informacji.



Zaprezentowany, powyższy wykres wskazuje na niewielkie rozbieżności, które wynikają z udzielonych przez wszystkich ankietowanych odpowiedzi. W celu zbadania tejże istotności wykonano test współczynnika korelacji liniowej r- Pearsona.

Tabela 4-8
Rozkład odpowiedzi dotyczący wprowadzenia w PSP procedur – polityki bezpieczeństwa informacji.

Odpowiedzi	I Grupa KW	II Grupa KM/KP	Ogółem		
	x_i	y_i	x_i^2	y_i^2	$x_i * y_i$
tak	332	1408	110224	1982464	467456
nie	14	104	196	10816	1456
nie wiem	6	33	36	1089	198
Ogółem	$\sum_{i=3}^{n} x_i =$ 352	$\sum_{i=3}^{n} y_i =$ 1545	$\sum_{i=3}^{n} x_i^2 =$ 110456	$\sum_{i=3}^{n} y_i^2 =$ 1994369	$\sum_{i=3}^{n} x_i * y_i =$ 469110
$\bar{x} = \frac{1}{n}\sum_{i=n}^{n} x_i = \frac{1}{3} * 352 \approx 117$ $x^2 \approx 13689$ | $\bar{y} = \frac{1}{n}\sum_{i=n}^{n} y_i = \frac{1}{3} * 1545 \approx 509$ $y^2 \approx 259\,081$					

Źródło: Opracowanie własne.

$$r = \frac{\frac{1}{n}\sum_{i=n}^{n} x_i y_i - xy}{\sqrt{(\frac{1}{n}\sum_{i=n}^{n} x_i^2 - x^2)(\frac{1}{n}\sum_{i=n}^{n} y_i^2 - y^2)}} = \frac{\frac{1}{3} * 469110 - 59044}{\sqrt{(\frac{1}{3} * 110456 - 13689)(\frac{1}{3} * 1994369 - 259081)}} \approx 0{,}99$$

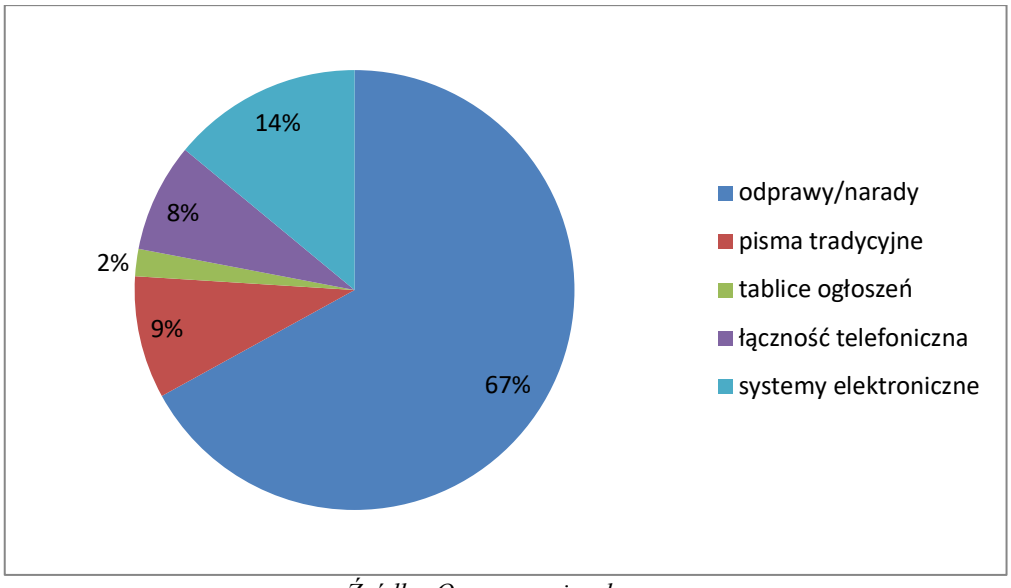
Podobnie jak w przypadku wcześniejszych pytań po przeprowadzeniu testu współczynnika korelacji liniowej r- Pearsona, otrzymano wynik r ≈ 0,99, co świadczy, że pomiędzy poszczególnymi grupami występuje bardzo silna zależność i mówimy o korelacji dodatniej. Wyniki świadczą o tym, iż wzrost wartości w odpowiedziach u jednej z grup powoduje wzrost wartości odpowiedzi w grupie drugiej.

W ramach przeprowadzonych badań empirycznych poproszono opiniodawców o udzielenie odpowiedzi na pytanie piąte (zał. 1): *5. Która z niżej wymienionych form komunikacji w Pani/Pana macierzystej jednostce PSP jest najskuteczniejsza?*

Respondenci standardowo mogli wybrać jedną możliwość spośród pięciu zaproponowanych wariantów, a dokładniej: odprawy/narady służbowe; pisma tradycyjne; tablice ogłoszeń; łączność telefoniczna; systemy elektroniczne (wideokonferencyjne i internetowe). Ogólny rozkład odpowiedzi został zilustrowany na wykresie 4-9, z analizy którego wynika, iż wśród wszystkich respondentów biorących udział w badaniu stwierdzono, że, najskuteczniejszą formą komunikacji w PSP są odprawy/narady służbowe, czego dowodem jest uzyskana liczba wskazań na tą odpowiedź na poziomie 67 % (1278 wskazań). Na drugim miejscu wśród odpowiedzi respondenci wskazali systemy elektroniczne 14 % (260 wskazań). Zaś kolejno praktycznie równorzędnie dwa zaproponowane warianty odpowiedzi, a mianowicie pisma tradycyjne oraz łączność telefoniczna. Te dwa warianty odpowiedzi uzyskały odpowiednio 9 % (163 wskazań) i 8 % (158 wskazań). Najmniej liczna część respondentów wskazała, iż to właśnie tablice ogłoszeń są najmniej skuteczną formą komunikacji, o czym świadczy uzyskanie 2 % głosów (38 wskazań).

Szczegółowy rozkład odpowiedzi został zilustrowany w tabeli 4-9.

Wykres 4-9
Procentowy rozkład odpowiedzi dotyczący skuteczności form komunikowania.



Źródło: Opracowanie własne.

Badani należący do pierwszej grupy najczęściej wskazywali na wariant odpowiedzi mówiący skuteczności w komunikacji odpraw i narad służbowych, o czym świadczy 62 % i 220 wskazań. Zdecydowanie mniej wskazań otrzymały kolejne propozycje odpowiedzi:

systemy elektroniczne 17 % - 62 wskazań; tradycyjne pisma 12 % - 38 wskazań; łączność telefoniczna 8 % - 28 wskazań. Natomiast odpowiedź tablice ogłoszeń uzyskały zaledwie 4 wskazania, co daje blisko 1 % odpowiedzi ogółu.

W drugiej grupie respondentów odpowiedzi rozłożyły się nieco inaczej, choć z zachowaniem podobnej tendencji jak w grupie I. Pierwszą odpowiedzią, analogicznie do pierwszej grupy, była największa ilość wskazań na narady i odprawy 68 % (1058 wskazań). Zdecydowanie mniej wskazań otrzymały kolejne propozycje odpowiedzi: systemy elektroniczne 13 % - 198 wskazań; łączność telefoniczna 9 % - *130* wskazań; tradycyjne pisma 8 % - 125 wskazań; Natomiast odpowiedź tablice ogłoszeń uzyskały tylko 34 wskazania, co daje niespełna 2 % całości odpowiedzi.

Szczegółowy rozkład odpowiedzi dotyczący występujących zagrożeń zaprezentowano w tabeli 4-9.

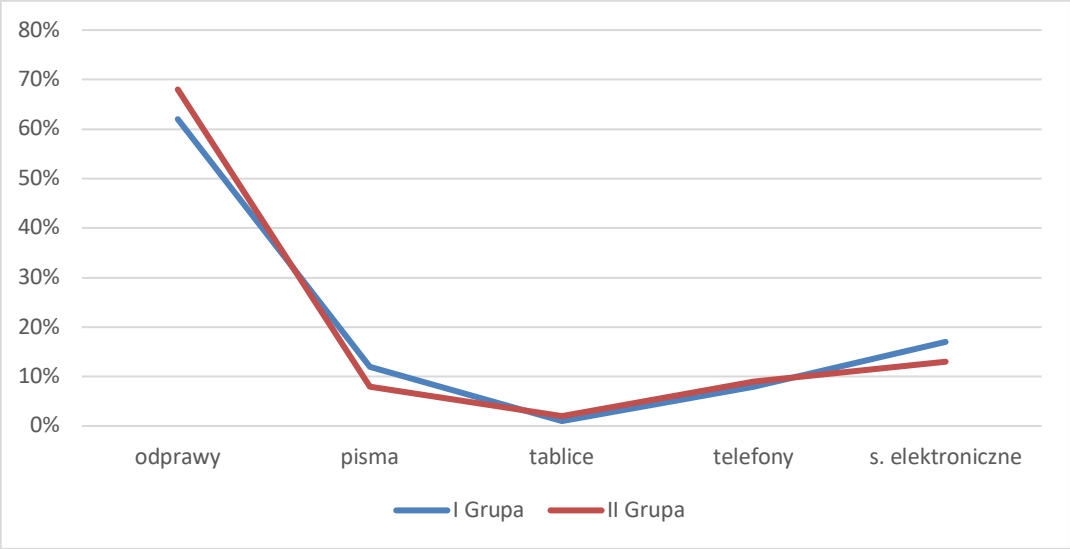
Tabela 4-9
Procentowy rozkład odpowiedzi dotyczący skuteczności form komunikowania.

Odpowiedzi	I Grupa PRACOWNICY KW		II Grupa PRACOWNICY KM/KP		Ogółem	
	Struktura liczbowa	Struktura procentowa (%)	Struktura liczbowa	Struktura procentowa (%)	Struktura liczbowa	Struktura procentowa (%)
odprawy/narady	220	62	1058	68	1278	67
pisma tradycyjne	38	12	125	8	163	9
tablice ogłoszeń	4	1	34	2	38	2
łączność telefoniczna	28	8	130	9	158	8
systemy elektroniczne	62	17	198	13	260	14
Ogółem	352	100	1545	100	1897	100

Źródło: Opracowanie własne.

W celu dokładniejszego zobrazowania uzyskanych rozkładów udzielonych odpowiedzi z obu grup, wyniki zaprezentowano na wykresie 4-10.

Wykres 4-10
Procentowy rozkład odpowiedzi w obu grupach badawczych dotyczący priorytetów podczas długotrwałych akcji ratowniczych.



Zaprezentowany, powyższy wykres wskazuje na niewielkie rozbieżności, które wynikają z udzielonych przez wszystkich ankietowanych odpowiedzi. W celu zbadania tejże istotności wykonano test współczynnika korelacji liniowej r- Pearsona.

Tabela 4-10
Rozkład odpowiedzi dotyczący skuteczności form komunikowania.

Odpowiedzi	**I Grupa Pracownicy KW**	**II Grupa Pracownicy KM/KP**	**Ogółem**		
	x_i	y_i	x_i^2	y_i^2	$x_i * y_i$
odprawy/narady	220	1058	48400	1119364	232760
pisma tradycyjne	38	125	1444	15625	4750
tablice ogłoszeń	4	34	16	1156	136
łączność telefoniczna	28	130	784	16900	3640
systemy elektroniczne	62	198	48400	1119364	232760
Ogółem	$\sum_{i=5}^{n} x_i =$ 352	$\sum_{i=5}^{n} y_i =$ 1545	$\sum_{i=5}^{n} x_i^2 =$ 50644	$\sum_{i=5}^{n} y_i^2 =$ 1153045	$\sum_{i=5}^{n} x_i * y_i =$ 241286

$\bar{x} = \frac{1}{n}\sum_{i=n}^{n} x_i = \frac{1}{5} * 352 \approx 70$ $x^2 = 4900$ $|\bar{y} = \frac{1}{n}\sum_{i=n}^{n} y_i = \frac{1}{5} * 1545 = 309$ $y^2 = 95\,481$

Źródło: Opracowanie własne.

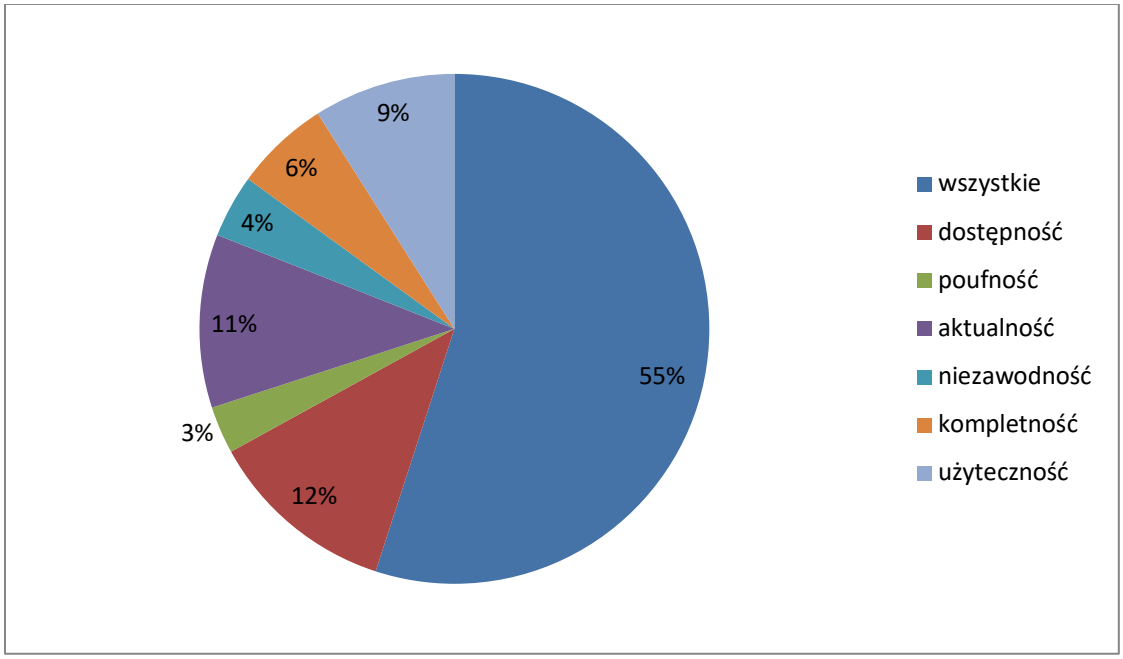
$$r = \frac{\frac{1}{n}\sum_{i=n}^{n} x_i y_i - xy}{\sqrt{(\frac{1}{n}\sum_{i=n}^{n} x_i^2 - x^2)(\frac{1}{n}\sum_{i=n}^{n} y_i^2 - y^2)}} = \frac{\frac{1}{5} * 241286 - 21\,630}{\sqrt{(\frac{1}{5} * 50644 - 4900)(\frac{1}{5} * 1153045 - 95481)}} = 1$$

Przedstawiona powyższa analiza ukazuje, że współczynnik korelacji liniowej Pearsona wynosi 1, co wskazuje na korelacje dodatnią o bardzo silnej zależności. Świadczy to o tym, iż wzrost wartości w udzielonych odpowiedziach jednej z grup powoduje wzrost wartości odpowiedzi drugiej z grup.

W ramach przeprowadzonych badań empirycznych poproszono respondentów o udzielenie odpowiedzi na pytanie szóste (zał. 1): 6. *Która z poniższych cech informacji Pani/Pana zdaniem jest najważniejsza/ma największy wpływ na skuteczne funkcjonowanie organizacji?*

Ankietowani mieli do wyboru sześć wariantów odpowiedzi, z których wybierali tylko jedną odpowiedź, co przełożyło się na uzyskanie 1897 wskazań. Ogólny rozkład odpowiedzi został zilustrowany na wykresie 4-11, z którego wynika, iż najwięcej wskazań otrzymała ostatnia zaproponowana możliwość, dotycząca wskazania, że wszystkie wskazane w odpowiedziach cechy informacji uznawane są przez respondentów za istotne w funkcjonowaniu organizacji. Procentowy udział wskazujących tą odpowiedź osób kształtuje się na poziomie 55 %, co stanowi 1033 wskazań respondentów obu grup. Kolejno najwięcej ankietowanych wskazało: dostępność 12 % (233 wskazania), aktualność 11% (201 wskazań), użyteczność 9 % (165 wskazania), kompletność 6 % (116 wskazań), niezawodność 4 % (78 wskazań), poufność 3 % (71 wskazań).

Wykres 4-11
Procentowy rozkład odpowiedzi dotyczący ważności cech informacji.



Źródło: Opracowanie własne.

Badani należący do I grupy, najczęściej wskazywali na wariant odpowiedzi mówiący, że wszystkie wskazane w odpowiedziach cechy informacji uznawane są przez respondentów za istotne w funkcjonowaniu organizacji. Procentowy udział wskazujących tą odpowiedź osób kształtuje się na poziomie 59 %, co stanowi 207 wskazań. Następnie najwięcej ankietowanych wskazało następujące warianty odpowiedzi: dostępność 11 % (40 wskazań), aktualność 11 % (40 wskazań), użyteczność 7 % (18 wskazania), kompletność 5 % (17 wskazań), niezawodność 4 % (15 wskazań), poufność 3 % (10 wskazań).

Bardzo podobnie ukształtował się rozkład odpowiedzi w II grupie badanych. Odpowiedź, że wszystkie wskazane w odpowiedziach cechy informacji uznawane są przez respondentów za istotne w funkcjonowaniu organizacji kształtuje się na poziomie 53 %, co stanowi 826 wskazań. Kolejno najwięcej ankietowanych wskazało następujące warianty odpowiedzi: dostępność 13 % (192 wskazań), aktualność 11 % (160 wskazań), użyteczność 9 % (146 wskazania), kompletność 6 % (98 wskazań), niezawodność 4 % (62 wskazań), poufność 4 % (61 wskazań).

Szczegółowy rozkład odpowiedzi dotyczący występujących zagrożeń zaprezentowano w tabeli 4-11

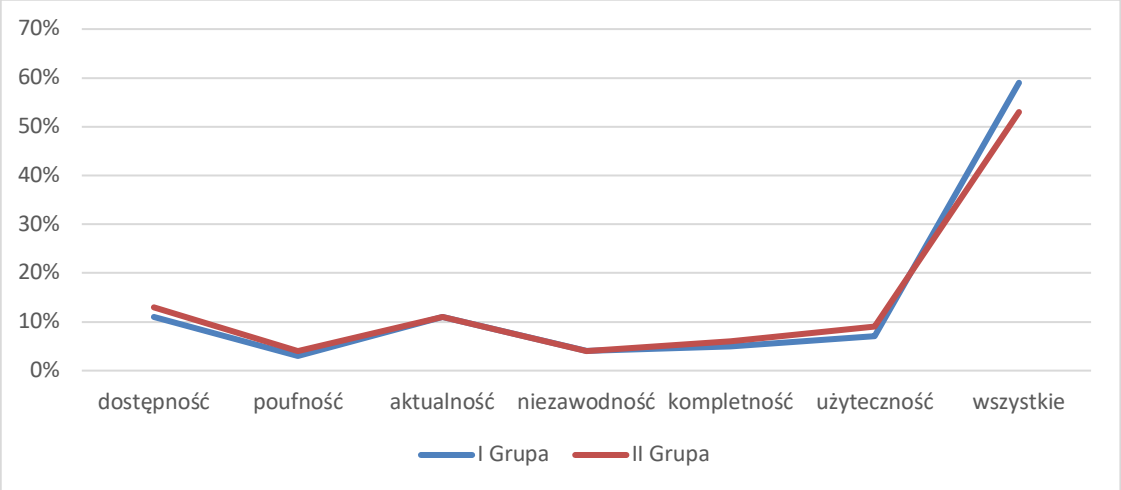
Tabela 4-11
Procentowy rozkład odpowiedzi dotyczący ważności cech informacji.

Odpowiedzi	I Grupa PRACOWNICY KW		II Grupa PRACOWNICY KM/KP		Ogółem	
	Struktura liczbowa	Struktura procentowa (%)	Struktura liczbowa	Struktura procentowa (%)	Struktura liczbowa	Struktura procentowa (%)
dostępność	40	11	192	13	233	12
poufność	10	3	61	4	71	3
aktualność	40	11	160	11	201	11
niezawodność	15	4	62	4	78	4
kompletność	17	5	98	6	116	6
użyteczność	18	7	146	9	165	7
wszystkie powyżej	207	59	826	53	1033	54
Ogółem	352	100	1545	100	1897	100

Źródło: Opracowanie własne.

W celu dokładniejszego zobrazowania uzyskanych rozkładów udzielonych odpowiedzi z obu grup, wyniki zaprezentowano na wykresie 4-12.

Wykres 4-12
Procentowy rozkład odpowiedzi w obu grupach badawczych dotyczący ważności cech informacji.



Zaprezentowany, powyższy wykres wskazuje na niewielkie rozbieżności, które wynikają z udzielonych przez wszystkich ankietowanych odpowiedzi. W celu zbadania tejże istotności wykonano test współczynnika korelacji liniowej r- Pearsona.

Tabela 4-12
Rozkład odpowiedzi dotyczący skuteczności form komunikowania.

Odpowiedzi	I Grupa KW	II Grupa KM/KP	Ogółem		
	x_i	y_i	x_i^2	y_i^2	$x_i * y_i$
dostępność	40	192	1600	36864	7680
poufność	10	61	100	3721	610
aktualność	40	160	1600	25600	6400
niezawodność	15	62	225	3844	930
kompletność	17	98	289	9604	1666
użyteczność	18	146	324	21316	2628
wszystkie powyżej	207	826	42849	682276	170982
Ogółem	$\sum_{i=5}^{n} x_i =$ 352	$\sum_{i=5}^{n} y_i =$ 1545	$\sum_{i=5}^{n} x_i^2 =$ 46987	$\sum_{i=5}^{n} y_i^2 =$ 783225	$\sum_{i=5}^{n} x_i * y_i =$ 190896
$\bar{x} = \frac{1}{n}\sum_{i=n}^{n} x_i = \frac{1}{7} * 352 \approx 50$ $x^2 = 2500$ $\bar{y} = \frac{1}{n}\sum_{i=n}^{n} y_i = \frac{1}{7} * 1545 \approx 221$ $y^2 = 48841$					

Źródło: Opracowanie własne.

$$r = \frac{\frac{1}{n}\sum_{i=n}^{n} x_i y_i - xy}{\sqrt{(\frac{1}{n}\sum_{i=n}^{n} x_i^2 - x^2)(\frac{1}{n}\sum_{i=n}^{n} y_i^2 - y^2)}} = \frac{\frac{1}{7} * 190896 - 11\,050}{\sqrt{(\frac{1}{7} * 46987 - 2500)(\frac{1}{7} * 783225 - 48841)}} = 0{,}99$$

Przedstawiona powyższa analiza ukazuje, że współczynnik korelacji liniowej Pearsona wynosi 0,99, co wskazuje na korelacje dodatnią o bardzo silnej zależności. Świadczy to o tym, iż wzrost wartości w udzielonych odpowiedziach jednej z grup powoduje wzrost wartości odpowiedzi drugiej z grup.

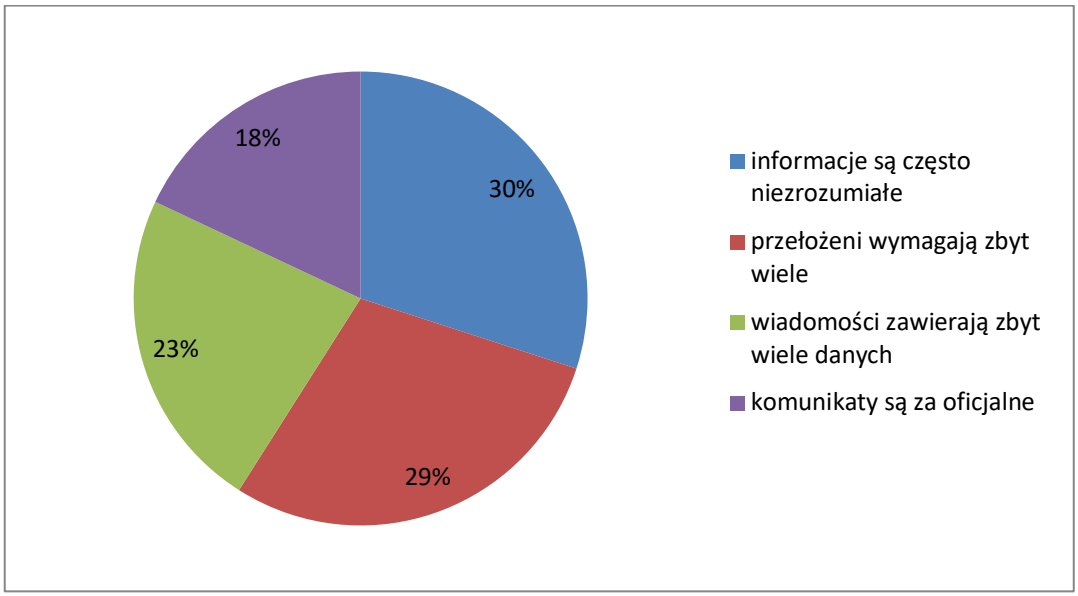
W ramach przeprowadzonych badań empirycznych poproszono respondentów o udzielenie odpowiedzi na pytanie siódme (zał. 1): *7. Który z niżej wymienionych elementów komunikacji uważa Pani/Pan za najczęściej spotykany błąd w PSP?*

Badanym zaproponowano cztery warianty odpowiedzi, jednokrotnego wyboru. Ogólny rozkład odpowiedzi został zaprezentowany na wykresie 4-13, z którego wynika, iż najwięcej opiniodawców odpowiedziało się za wariantem, że przekazywane informacje są często niezrozumiałe dla adresata 30 % z 566 wskazaniami. Następnie wskazywano, iż przełożeni wymagają zbyt wiele i nie reagują na sugestie podwładnych 29 % z 564 wskazaniami, kolejno uplasowała się odpowiedź, że przekazywane wiadomości zawierają zbyt wiele danych interesujących kierownictwo, a nie pracowników 23 %

z 435 wskazaniami i na końcu odpowiedź, że komunikaty są za oficjalne, w jednostce jest zbyt mało otwartości i szczerości 18 % z 332 wskazaniami.

Szczegółowy rozkład został ujęty w tabeli 4-13.

Wykres 4-13
Procentowy rozkład odpowiedzi dotyczący błędów w komunikacji w PSP.



Źródło: Opracowanie własne.

W rozbiciu na poszczególne grupy respondentów odpowiedzi kształtowały się następująco. Ankietowani należący do I grupy najczęściej wskazywali na odpowiedź, że przekazywane informacje są często niezrozumiałe dla adresata - odpowiedź ta uzyskała 32%, co stanowiło 111 wskazania. Na drugim miejscu uplasował się wariant odpowiedzi, iż przełożeni wymagają zbyt wiele i nie reagują na sugestie podwładnych, gdzie wskazania takiego dokonało 97 respondentów – 27 %. Trzecim wariantem została odpowiedź, że komunikaty są za oficjalne, w jednostce jest zbyt mało otwartości i szczerości, na którą zdecydowało się 80 ankietowanych - 23 %. Na ostatnim miejscu ankietowani wskazali, że przekazywane wiadomości zawierają zbyt wiele danych interesujących kierownictwo, a nie pracowników 64 wskazania, co daje 18 % całości odpowiedzi.

W II grupie ankietowanych największa część respondentów zdecydowała się na odpowiedź, że przełożeni wymagają zbyt wiele i nie reagują na sugestie podwładnych, 468 wskazań – 30 %. Wariant odpowiedzi, że przekazywane informacje są często niezrozumiałe dla adresata wybrało 454 respondentów – 29 %. Natomiast trzecim wyborem w tej grupie została odpowiedź przekazywane wiadomości zawierają zbyt wiele danych interesujących kierownictwo, a nie pracowników, na którą zdecydowało się 371 ankietowanych

- 25 %. Najrzadziej wybieraną odpowiedzią wśród ankietowanych dotyczącą tego pytania była odpowiedź komunikaty są za oficjalne, w jednostce jest zbyt mało otwartości i szczerości, którą wybrało 252 osób - 16 %.

Szczegółowy rozkład danych odpowiedzi został ukazany w tabeli 4-13

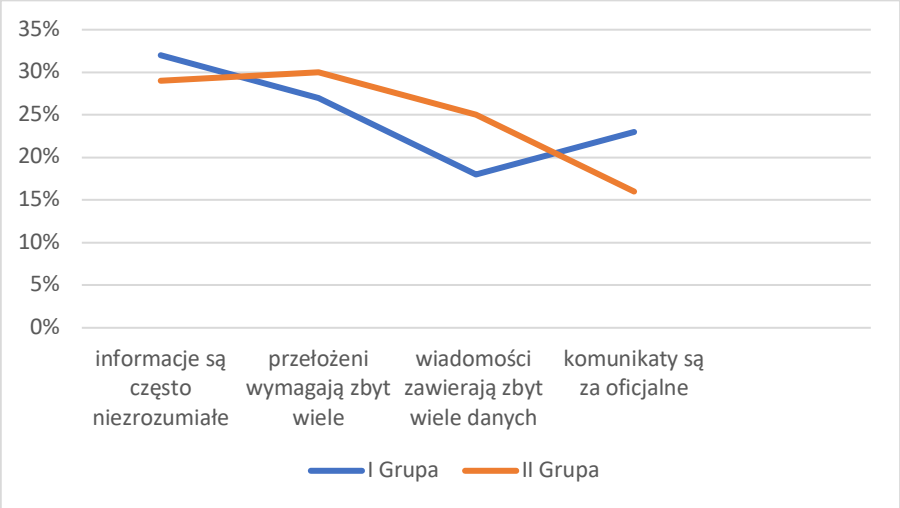
Tabela 4-13
Procentowy rozkład odpowiedzi dotyczący błędów w komunikacji w PSP.

Odpowiedzi	I Grupa PRACOWNICY KW		II Grupa PRACOWNICY KM/KP		Ogółem	
	Struktura liczbowa	Struktura procentowa (%)	Struktura liczbowa	Struktura procentowa (%)	Struktura liczbowa	Struktura procentowa (%)
informacje są często niezrozumiałe	111	32	454	29	1620	85
przełożeni wymagają zbyt wiele	97	27	468	30	119	7
wiadomości zawierają zbyt wiele danych	64	18	371	25	112	6
komunikaty są za oficjalne	80	23	252	16	7	2
Ogółem	352	100	1545	100	1897	100

Źródło: Opracowanie własne.

W celu dokładniejszego zobrazowania uzyskanych rozkładów udzielonych odpowiedzi z obu grup, wyniki zaprezentowano na wykresie 4-14.

Wykres 4-14
Procentowy rozkład odpowiedzi w obu grupach badawczych dotyczący błędów w komunikacji w PSP



Zaprezentowany, powyższy wykres wskazuje na rozbieżności, które wynikają z udzielonych przez wszystkich ankietowanych odpowiedzi. W celu zbadania tejże istotności wykonano test współczynnika korelacji liniowej r- Pearsona.

Tabela 4-14
Rozkład odpowiedzi dotyczący błędów w komunikacji w PSP

Odpowiedzi	I Grupa KW	II Grupa KM/KP	Ogółem		
	x_i	y_i	x_i^2	y_i^2	$x_i * y_i$
informacje są często niezrozumiałe	111	454	12321	206116	50394
przełożeni wymagają zbyt wiele	97	468	9409	219024	45396
wiadomości zawierają zbyt wiele danych	64	371	4096	137641	23744
komunikaty są za oficjalne	80	252	6400	63504	20160
Ogółem	$\sum_{i=3}^{n} x_i =$ 352	$\sum_{i=3}^{n} y_i =$ 1545	$\sum_{i=3}^{n} x_i^2 =$ 32226	$\sum_{i=3}^{n} y_i^2 =$ 626285	$\sum_{i=3}^{n} x_i * y_i =$ 139694
$\bar{x} = \frac{1}{n}\sum_{i=n}^{n} x_i = \frac{1}{4} * 352 \approx 88$ $x^2 \approx 7\,744$ | $\bar{y} = \frac{1}{n}\sum_{i=n}^{n} y_i = \frac{1}{4} * 1545 \approx 386$ $y^2 \approx 148\,996$					

Źródło: Opracowanie własne.

$$r = \frac{\frac{1}{n}\sum_{i=n}^{n} x_i y_i - xy}{\sqrt{(\frac{1}{n}\sum_{i=n}^{n} x_i^2 - x^2)(\frac{1}{n}\sum_{i=n}^{n} y_i^2 - y^2)}} = \frac{\frac{1}{4} * 139694 - 33\,968}{\sqrt{(\frac{1}{4} * 32226 - 7\,744)(\frac{1}{4} * 626285 - 148\,996)}} \approx 0{,}61$$

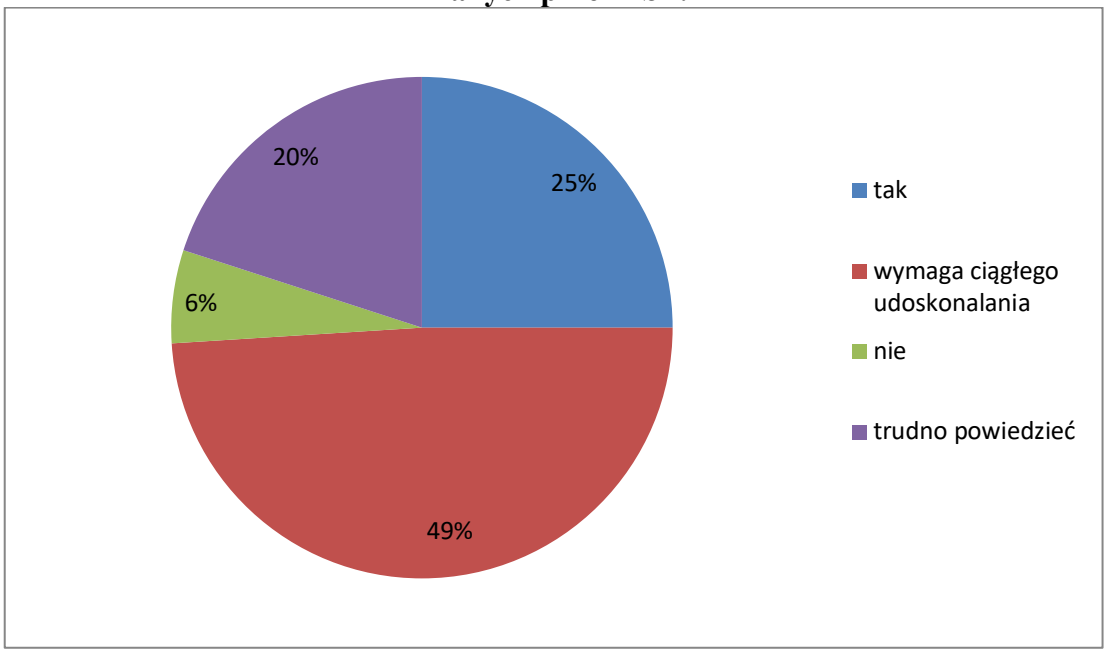
Powyższy wynik współczynnika korelacji liniowej r- Pearsona wynosi r≈0,61, co świadczy o korelacji dodatniej o umiarkowanym stopniu. tzn. że tylko część danych spełnia zależność – tendencja jest widoczna, ale zdarza się więcej odstępstw niż w przypadku silniejszej zależności.

W ramach przeprowadzonych badań empirycznych poproszono opiniodawców o udzielenie odpowiedzi na pytanie ósme (zał. 1): 8. *Czy według Pani/Pan system informacyjny PSP w pełni chroni informacje pozyskiwane i przetwarzane przez tą formację?*

Respondenci mogli wybrać zaledwie jedną możliwość spośród czterech zaproponowanych wariantów, a dokładniej: tak; częściowo tak - ale wymaga ciągłego udoskonalania; nie oraz trudno powiedzieć. Ogólny rozkład odpowiedzi został zilustrowany na wykresie 4-15, z analizy którego wynika, iż odpowiedź częściowo tak - ale wymaga ciągłego udoskonalania była zdecydowanie najczęściej wybieraną odpowiedzią wśród wszystkich respondentów biorących udział w badaniu, czego dowodem jest uzyskana liczba wskazań na tą odpowiedź na poziomie 49 % (928 wskazań). Na drugim miejscu wśród odpowiedzi respondenci wskazali odpowiedź na tak, która uzyskała 25 %, na co złożyło się odpowiednio 477 wskazań. Kolejna część respondentów wskazała, iż trudno powiedzieć, na co złożyło się uzyskanie 20 % poparcia (380 wskazań) i na ostatnim miejscu wybierano odpowiedź nie z 112 wskazaniami i 6 % wyborów.

Szczegółowy rozkład odpowiedzi został zilustrowany w tabeli 4-15.

Wykres 4-15
Procentowy rozkład odpowiedzi dotyczący poprawności ochrony informacji przetwarzanych przez PSP.



Źródło: Opracowanie własne.

Badani należący do I grupy najczęściej wskazywali na wariant odpowiedzi mówiący o tym, że system informacyjny częściowo chroni zasoby PSP i wymaga ciągłego udoskonalania o czym świadczy 173 wskazania i wynik 49 %. Mniej wskazań otrzymały kolejne propozycje odpowiedzi: tak 89 wskazań i 25 %, trudno powiedzieć 75 wskazania i 22 %. Natomiast odpowiedź nie uzyskała zaledwie 15 wskazań, co daje 4 %.

Podobnie ukształtował się rozkład wyników II grupy respondentów. Ankietowani najczęściej dokonywali wyboru tak jak w I grupie mówiący o potrzebie ciągłego doskonalenia systemu, uzyskano odpowiedzi na poziomie 49 % (755 wskazań). Kolejną wybieraną w tej grupie była odpowiedź tak na poziomie 25 % i 388 wskazań. Na trzecim miejscu respondenci tej grupy wskazali odpowiedź trudno powiedzieć z 305 wskazaniami i 20 %. Na ostatnim miejscu wskazywano odpowiedź nie z 97 wskazaniami, co daje 6 % odpowiedzi.

Szczegółowy rozkład odpowiedzi dotyczący występujących zagrożeń zaprezentowano w tabeli 4-15

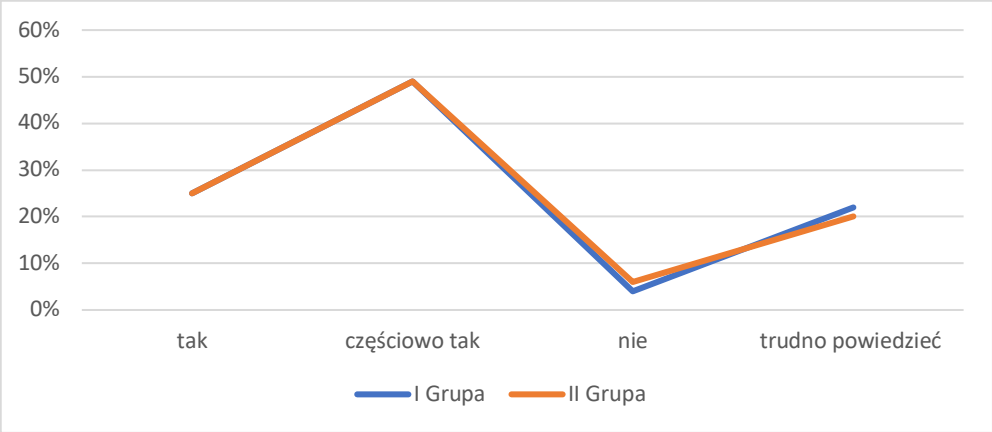
Tabela 4-15
Procentowy rozkład odpowiedzi dotyczący poprawności ochrony informacji przetwarzanych przez PSP.

Odpowiedzi	I Grupa PRACOWNICY KW		II Grupa PRACOWNICY KM/KP		Ogółem	
	Struktura liczbowa	Struktura procentowa (%)	Struktura liczbowa	Struktura procentowa (%)	Struktura liczbowa	Struktura procentowa (%)
tak	89	25	388	25	477	25
częściowo tak- wymaga udoskonalania	173	49	755	49	928	49
nie	15	4	97	6	112	6
trudno powiedzieć	75	22	305	20	380	20
Ogółem	352	100	1545	100	1897	100

Źródło: Opracowanie własne.

W celu dokładniejszego zobrazowania uzyskanych rozkładów udzielonych odpowiedzi z obu grup, wyniki zaprezentowano na wykresie 4-16.

Wykres 4-16
Procentowy rozkład odpowiedzi w obu grupach badawczych dotyczący poprawności ochrony informacji przetwarzanych przez PSP.



Zaprezentowany, powyższy wykres wskazuje na niewielkie rozbieżności, które wynikają z udzielonych przez wszystkich ankietowanych odpowiedzi. W celu zbadania tejże istotności wykonano test współczynnika korelacji liniowej r- Pearsona.

Tabela 4-16
Rozkład odpowiedzi dotyczący poprawności ochrony informacji przetwarzanych przez PSP.

Odpowiedzi	**I Grupa KW**	**II Grupa KM/KP**	**Ogółem**		
	x_i	y_i	x_i^2	y_i^2	$x_i * y_i$
Tak	89	388	7921	150544	34532
częściowo tak- wymaga udoskonalania	173	755	29929	570025	130615
Nie	15	97	225	9409	1455
trudno powiedzieć	75	305	5625	93025	22875
Ogółem	$\sum_{i=3}^{n} x_i =$ 352	$\sum_{i=3}^{n} y_i =$ 1545	$\sum_{i=3}^{n} x_i^2 =$ 43700	$\sum_{i=3}^{n} y_i^2 =$ 823003	$\sum_{i=3}^{n} x_i * y_i =$ 189477
$\bar{x} = \frac{1}{n}\sum_{i=n}^{n} x_i = \frac{1}{4} * 352 \approx 88$ $x^2 \approx 7\,744$ | $\bar{y} = \frac{1}{n}\sum_{i=n}^{n} y_i = \frac{1}{4} * 1545 \approx 386$ $y^2 \approx 148\,996$					

Źródło: Opracowanie własne.

$$r = \frac{\frac{1}{n}\sum_{i=n}^{n} x_i y_i - xy}{\sqrt{(\frac{1}{n}\sum_{i=n}^{n} x_i^2 - x^2)(\frac{1}{n}\sum_{i=n}^{n} y_i^2 - y^2)}} = \frac{\frac{1}{4} * 189477 - 33\,968}{\sqrt{(\frac{1}{4} * 43700 - 7\,744\,)(\frac{1}{4} * 823003 - 148\,996)}} \approx 0{,}99$$

Przedstawiona powyższa analiza ukazuje, że współczynnik korelacji liniowej Pearsona wynosi 0,99, co wskazuje na korelacje dodatnią o bardzo silnej zależności. Świadczy

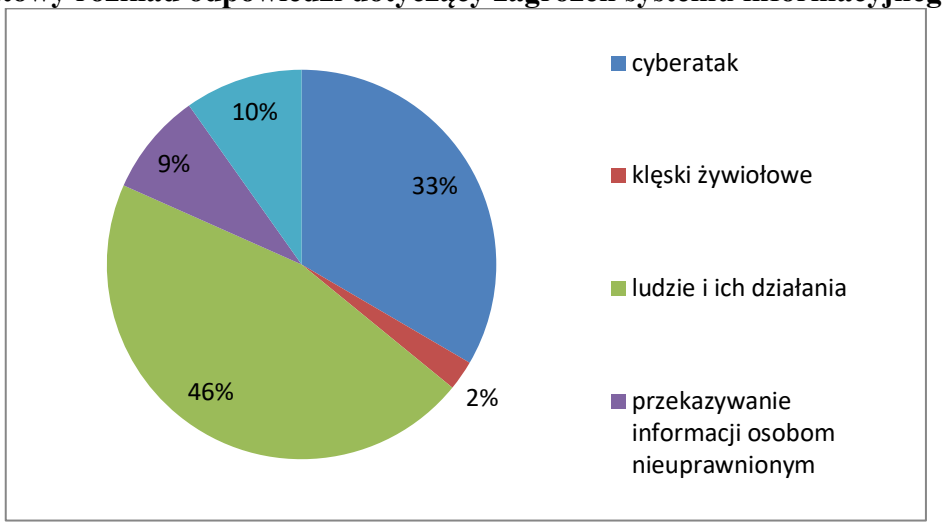
to o tym, iż wzrost wartości w udzielonych odpowiedziach jednej z grup powoduje wzrost wartości odpowiedzi drugiej z grup.

W ramach przeprowadzonych badań empirycznych poproszono respondentów o udzielenie odpowiedzi na kolejne dziewiąte pytanie (zał. 1): 9. *Które z niżej wymienionych zagrożeń jest Pani/Pan zdaniem najpoważniejsze dla systemu informacyjnego w PSP?*

Respondenci mogli wybrać jedną możliwą odpowiedź spośród pięciu zaproponowanych wariantów: ludzie i ich działania (świadome, bądź nieświadome); klęski żywiołowe (pożar, katastrofy techniczne, zalanie pomieszczeń, itp.); wady techniczne sprzętu; cyberatak w tym wirusy, robaki, konie trojańskie; przekazywanie informacji osobom nieuprawnionym. Ogólny rozkład odpowiedzi został zilustrowany na wykresie 4-7, z analizy którego wynika, iż wśród wszystkich ankietowanych najczęściej wybierana była odpowiedź, że największym zagrożeniem systemu informacyjnego PSP są ludzie i ich działania (świadome, bądź nieświadome), czego dowodem jest uzyskana liczba 868 wskazań na tą odpowiedź na poziomie 46 %. Na drugim miejscu wśród odpowiedzi respondenci wskazali cyberatak w tym wirusy, robaki, konie trojańskie 33 % (634 wskazań). Kolejne odpowiedzi uzyskały stosunkowo niższe wyniki, a mianowicie: wady techniczne sprzętu 10 % (186 wskazań), przekazywanie informacji osobom nieuprawnionym 9 % (162 wskazań). Najmniej liczna część respondentów wskazała na odpowiedź klęski żywiołowe (pożar, katastrofy techniczne, zalanie pomieszczeń, itp.) 2 % głosów (38 wskazań).

Szczegółowy rozkład odpowiedzi został zilustrowany w tabeli 4-17.

Wykres 4-17
Procentowy rozkład odpowiedzi dotyczący zagrożeń systemu informacyjnego PSP.



Źródło: Opracowanie własne.

Badani należący do I grupy najczęściej wskazywali na wariant odpowiedzi mówiący, że największym zagrożeniem dla systemu informacyjnego są ludzie i ich działania, o czym świadczy 53 % i 186 wskazań. Następnie wskazywano cyberatak w tym wirusy, robaki, konie trojańskie 30 % - 108 wskazań, a potem równorzędnie wady techniczne sprzętu oraz przekazywanie informacji osobom nieuprawnionym po 8 % - 27 wskazań. Natomiast odpowiedź klęski żywiołowe uzyskały zaledwie 4 wskazania, co daje blisko 1 % odpowiedzi ogółu.

W II grupie respondentów odpowiedzi rozłożyły się nieco inaczej, choć z zachowaniem podobnej tendencji jak w grupie I. Pierwszą odpowiedzią, analogicznie do pierwszej grupy, była ludzie i ich działania 44 % (682 wskazań). Następnie cyberatak w tym wirusy, robaki, konie trojańskie 35 % - 525 wskazań i kolejno wady techniczne sprzętu 10 % - 160 wskazań; przekazywanie informacji osobom nieuprawnionym 9 % - 136 wskazań;. Natomiast odpowiedź klęski żywiołowe uzyskały tylko 42 wskazania, co daje niespełna 2 % całości odpowiedzi.

Szczegółowy rozkład odpowiedzi dotyczący występujących zagrożeń zaprezentowano w tabeli 4-17.

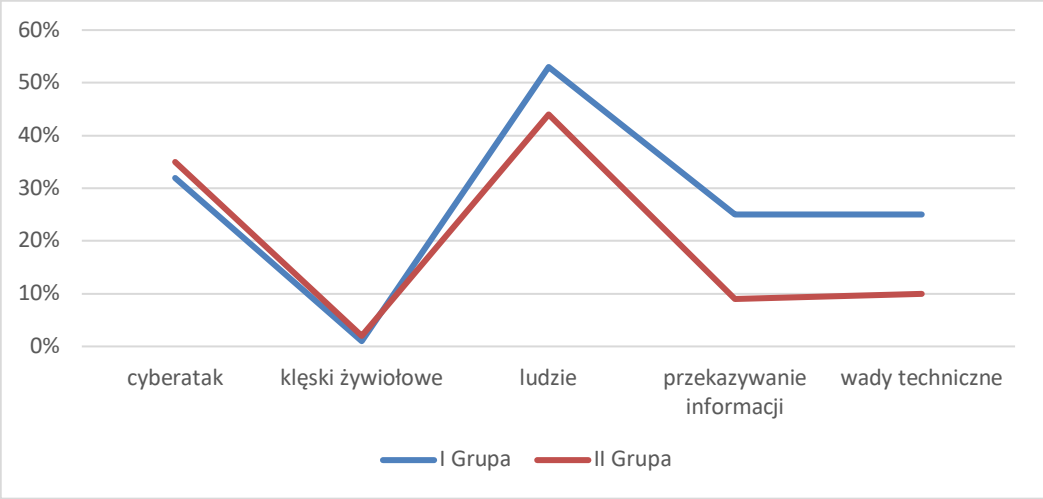
Tabela 4-17
Procentowy rozkład odpowiedzi dotyczący zagrożeń systemu informacyjnego PSP.

Odpowiedzi	I Grupa PRACOWNICY KW		II Grupa PRACOWNICY KM/KP		Ogółem	
	Struktura liczbowa	Struktura procentowa (%)	Struktura liczbowa	Struktura procentowa (%)	Struktura liczbowa	Struktura procentowa (%)
cyberatak	108	32	525	35	634	33
klęski żywiołowe	4	1	42	2	38	2
ludzie i ich działania	186	53	682	44	868	46
przekazywanie informacji osobom nieuprawnionym	27	8	136	9	162	9
wady techniczne sprzętu	27	8	160	10	186	10
Ogółem	352	100	1545	100	1897	100

Źródło: Opracowanie własne.

W celu dokładniejszego zobrazowania uzyskanych rozkładów udzielonych odpowiedzi z obu grup, wyniki zaprezentowano na wykresie 4-18.

Wykres 4-18
Procentowy rozkład odpowiedzi w obu grupach badawczych dotyczący zagrożeń systemu informacyjnego PSP.



Zaprezentowany, powyższy wykres wskazuje na niewielkie rozbieżności, które wynikają z udzielonych przez wszystkich ankietowanych odpowiedzi. W celu zbadania tejże istotności wykonano test współczynnika korelacji liniowej r- Pearsona.

Tabela 4-18
Rozkład odpowiedzi dotyczący zagrożeń systemu informacyjnego PSP.

Odpowiedzi	I Grupa KW	II Grupa KM/KP	Ogółem		
	x_i	y_i	x_i^2	y_i^2	$x_i * y_i$
cyberatak	108	525	11664	275625	56700
klęski żywiołowe	4	42	16	1764	168
ludzie i ich działania	186	682	34596	465124	126852
przekazywanie informacji osobom nieuprawnionym	27	136	729	18496	3672
wady techniczne sprzętu	27	160	729	25600	4320
Ogółem	$\sum_{i=5}^{n} x_i =$ 352	$\sum_{i=5}^{n} y_i =$ 1545	$\sum_{i=5}^{n} x_i^2 =$ 47734	$\sum_{i=5}^{n} y_i^2 =$ 786609	$\sum_{i=5}^{n} x_i * y_i =$ 191712

$\bar{x} = \frac{1}{n}\sum_{i=n}^{n} x_i = \frac{1}{5} * 352 \approx 70$ $x^2 = 4900$ $|\bar{y} = \frac{1}{n}\sum_{i=n}^{n} y_i = \frac{1}{5} * 1545 = 309$ $y^2 = 95\,481$

Źródło: Opracowanie własne.

$$r = \frac{\frac{1}{n}\sum_{i=n}^{n} x_i y_i - xy}{\sqrt{(\frac{1}{n}\sum_{i=n}^{n} x_i^2 - x^2)(\frac{1}{n}\sum_{i=n}^{n} y_i^2 - y^2)}} = \frac{\frac{1}{5} * 191712 - 21\,630}{\sqrt{(\frac{1}{5} * 47734 - 4900)(\frac{1}{5} * 786609 - 95481)}} = 0{,}98$$

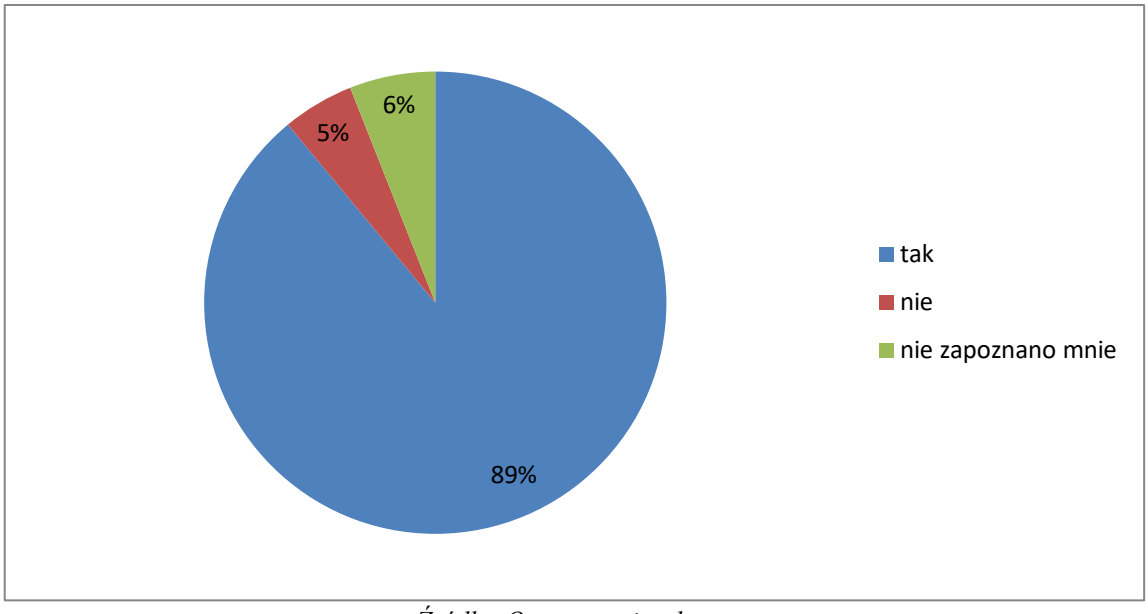
Przedstawiona powyższa analiza ukazuje, że współczynnik korelacji liniowej Pearsona wynosi r = 0,98, co wskazuje na korelacje dodatnią o bardzo silnej zależności. Świadczy to o tym, iż wzrost wartości w udzielonych odpowiedziach jednej z grup powoduje wzrost wartości odpowiedzi drugiej z grup.

W ramach przeprowadzonych badań empirycznych poproszono ankietowanych o udzielenie odpowiedzi na dziesiąte z rzędu pytanie (zał. 1): 10. *Czy posiada Pani/Pan świadomość konsekwencji o skutkach łamania zasad korzystania z systemu informacyjnego PSP i braku odpowiedzialności?*

Ogólny rozkład odpowiedzi został zaprezentowany na wykresie 4-19, z którego wynika, iż najwięcej opiniodawców odpowiedziało się za pierwszym wariantem odpowiedzi tak - potwierdzającym ich świadomość odpowiedzialności w tym zakresie, o czym świadczy 89 % uzyskanych odpowiedzi, na co złożyło się 1693 wskazań. Kolejne odpowiedzi uzyskały zdecydowanie mniejsze wyniki: nie 89 wskazań – 5 % i odpowiedź nie zapoznano mnie 112 wskazań – 6 % próby badawczej.

Szczegółowy rozkład odpowiedzi respondentów został ukazany w tabeli 4-19.

Wykres 4-19
Procentowy rozkład odpowiedzi dotyczący posiadania świadomości konsekwencji łamania zasad systemu informacyjnego w PSP.



Źródło: Opracowanie własne.

Badani należący do I grupy najczęściej wskazywali na wariant odpowiedzi tak – 89 % (314 wskazań), na drugim miejscu ukształtowała się odpowiedź nie zapoznano mnie z nimi – 6 % (22 wskazań) i dalej odpowiedź nie – 5 % (16 wskazań).

Identyczny rozkład wyników ukształtował się w II grupie respondentów. Ankietowani najczęściej dokonywali wyboru odpowiedzi tak – 89 % (1380 wskazań), kolejno padała odpowiedź nie zapoznano mnie z nimi – 6 % (91 wskazania) i na trzecim miejscu nie – 5 % (74 wskazań).

Szczegółowy rozkład odpowiedzi dotyczący świadomości konsekwencji naruszeń zasad korzystania z systemu informacyjnego w PSP został przedstawiony w tabeli 4-19.

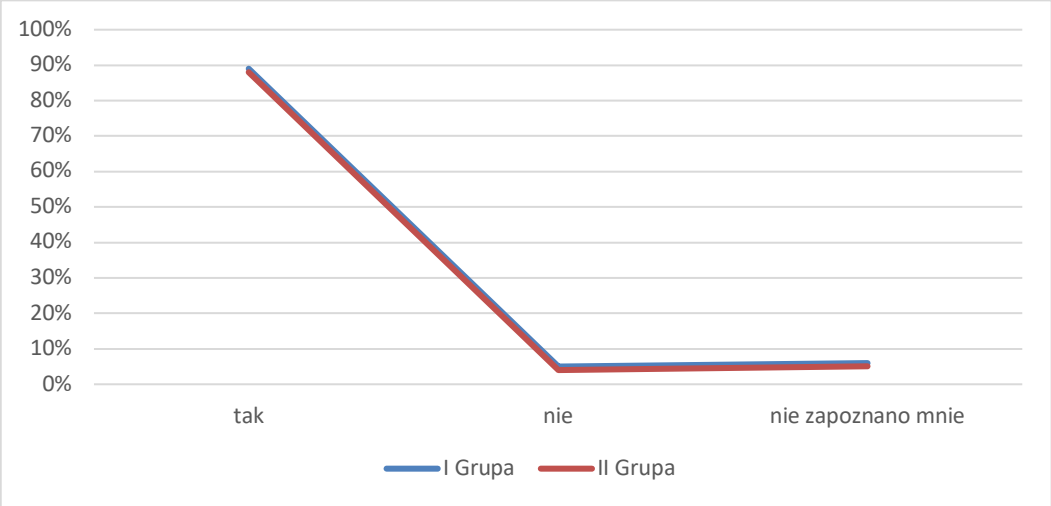
Tabela 4-19
Procentowy rozkład odpowiedzi dotyczący posiadania świadomości konsekwencji łamania zasad systemu informacyjnego w PSP.

Odpowiedzi	I Grupa PRACOWNICY KW		II Grupa PRACOWNICY KM/KP		Ogółem	
	Struktura liczbowa	Struktura procentowa (%)	Struktura liczbowa	Struktura procentowa (%)	Struktura liczbowa	Struktura procentowa (%)
tak	314	89	1380	89	1694	89
nie	16	5	74	5	90	5
nie zapoznano mnie	22	6	91	6	113	6
Ogółem	352	100	1545	100	1897	100

Źródło: Opracowanie własne.

W celu dokładniejszego zobrazowania uzyskanych rozkładów udzielonych odpowiedzi z obu grup, wyniki zaprezentowano na wykresie 4-20.

Wykres 4-20
Procentowy rozkład odpowiedzi w obu grupach badawczych dotyczący posiadania świadomości konsekwencji łamania zasad systemu informacyjnego w PSP.



Zaprezentowany, powyższy wykres wskazuje na niewielkie rozbieżności, które wynikają z udzielonych odpowiedzi przez uczestników obydwu grup. W celu zbadania tejże istotności wykonano test współczynnika korelacji liniowej r- Pearsona.

Tabela 4-20
Rozkład odpowiedzi dotyczący posiadania świadomości konsekwencji łamania zasad systemu informacyjnego w PSP.

Odpowiedzi	I Grupa KW	II Grupa KM/KP	Ogółem		
	x_i	y_i	x_i^2	y_i^2	$x_i * y_i$
Tak	314	1380	98596	1904400	433320
Nie	16	74	256	5476	1184
trudno powie-dzieć	22	91	484	8281	2002
Ogółem	$\sum_{i=3}^{n} x_i =$ 352	$\sum_{i=3}^{n} y_i =$ 1545	$\sum_{i=3}^{n} x_i^2 =$ 99336	$\sum_{i=3}^{n} y_i^2 =$ 1918157	$\sum_{i=3}^{n} x_i * y_i =$ 436506
$\bar{x} = \frac{1}{n}\sum_{i=n}^{n} x_i = \frac{1}{3} * 352 \approx 117$ $x^2 \approx 13689$ | $\bar{y} = \frac{1}{n}\sum_{i=n}^{n} y_i = \frac{1}{3} * 1545 \approx 509$ $y^2 \approx 259\,081$					

Źródło: Opracowanie własne.

$$r = \frac{\frac{1}{n}\sum_{i=n}^{n} x_i y_i - xy}{\sqrt{(\frac{1}{n}\sum_{i=n}^{n} x_i^2 - x^2)(\frac{1}{n}\sum_{i=n}^{n} y_i^2 - y^2)}} = \frac{\frac{1}{3} * 436506 - 59044}{\sqrt{(\frac{1}{3} * 99336 - 13689)(\frac{1}{3} * 1918157 - 259081)}} = 1$$

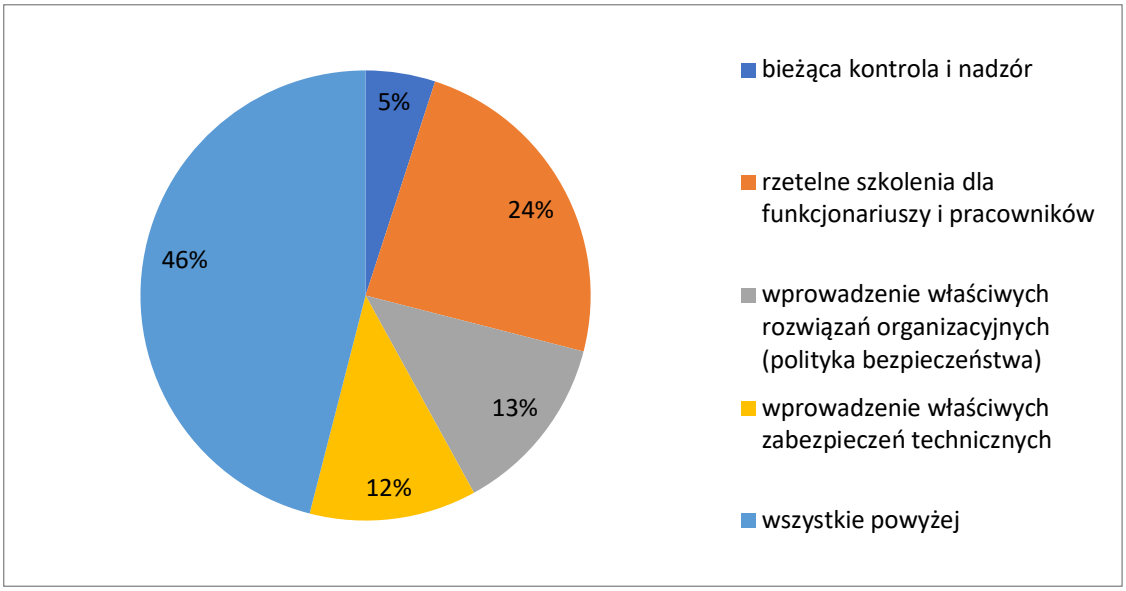
Po przeprowadzeniu testu współczynnika korelacji liniowej r- Pearsona, otrzymano wynik r = 1, co świadczy o tym, iż wzrost wartości w odpowiedziach u jednej z grup powoduje wzrost wartości odpowiedzi w grupie drugiej.

W ramach przeprowadzonych badań empirycznych poproszono opiniodawców o udzielenie odpowiedzi na pytanie jedenaste (zał. 1): 11. *Który z niżej wymienionych elementów Pani/Pana zdaniem ma decydujący wpływ na bezpieczeństwo systemu informacyjnego w PSP?*

Respondenci standardowo mogli wybrać tylko jedną możliwość spośród pięciu zaproponowanych w tym wariancie odpowiedzi, a dokładniej: bieżąca kontrola i nadzór, rzetelne szkolenia dla funkcjonariuszy i pracowników, wprowadzenie właściwych rozwiązań organizacyjnych (polityka bezpieczeństwa), wprowadzenie właściwych zabezpieczeń technicznych, wszystkie powyżej. Ogólny rozkład odpowiedzi został zilustrowany na wykresie 4-21, z analizy którego wynika, iż wśród wszystkich respondentów biorących udział w badaniu stwierdzono, że, decydujący i równorzędny wpływ na bezpieczeństwo systemu informacyjnego w PSP mają wszystkie czynniki wymienione w zaproponowanych odpowiedziach w tym pytaniu, czego dowodem jest uzyskana liczba wskazań na tą odpowiedź na poziomie 46 % (865 wskazań). Na drugim miejscu wśród odpowiedzi respondenci wskazali rzetelne szkolenia dla funkcjonariuszy i pracowników 24 % (463 wskazań). Zaś kolejno praktycznie równorzędnie dwa zaproponowane warianty odpowiedzi, a mianowicie wprowadzenie właściwych rozwiązań organizacyjnych (polityka bezpieczeństwa) oraz wprowadzenie właściwych zabezpieczeń technicznych. Te dwa warianty odpowiedzi uzyskały odpowiednio 13 % (247 wskazań) i 12 % (239 wskazań). Najmniej liczna część respondentów wskazała, iż to bieżąca kontrola i nadzór wpływają na bezpieczeństwo tego systemu, o czym świadczy uzyskanie 5 % głosów (83 wskazań).

Szczegółowy rozkład odpowiedzi został *zilustrowany* w tabeli 4-21.

Wykres 4-21
Procentowy rozkład odpowiedzi dotyczący elementów bezpieczeństwa systemu informacyjnego PSP.



Źródło: Opracowanie własne.

Badani należący do I grupy najczęściej wskazywali na wariant odpowiedzi mówiący, że wszystkie czynniki są decydujące, o czym świadczy 48 % i 169 wskazań. Mniej wskazań otrzymały kolejne propozycje odpowiedzi: rzetelne szkolenia dla funkcjonariuszy i pracowników 30 % - 107 wskazań; wprowadzenie właściwych zabezpieczeń technicznych 9 % - 32 wskazań; wprowadzenie właściwych rozwiązań organizacyjnych 9 % - 31 wskazań. Natomiast odpowiedź bieżąca kontrola i nadzór uzyskały tylko 13 wskazań, co daje 4 % odpowiedzi ogółu.

W drugiej grupie respondentów odpowiedzi rozłożyły się nieco nieznacznie inaczej. Podobnie jak w grupie I pierwszą wskazywaną odpowiedzią była, że wszystkie czynniki są decydujące 45 % (696 wskazań). Zdecydowanie mniej wskazań otrzymały kolejne propozycje odpowiedzi: rzetelne szkolenia dla funkcjonariuszy i pracowników 23 % - 356 wskazań; wprowadzenie właściwych rozwiązań organizacyjnych 14 % - 216 wskazań; wprowadzenie właściwych zabezpieczeń technicznych 13 % - 207 wskazań. Podobnie jak w I grupie odpowiedź bieżąca kontrola i nadzór uzyskała najmniej wskazań 70, co daje niespełna 5 % całości odpowiedzi.

Szczegółowy rozkład odpowiedzi dotyczący występujących zagrożeń zaprezentowano w tabeli 4-21.

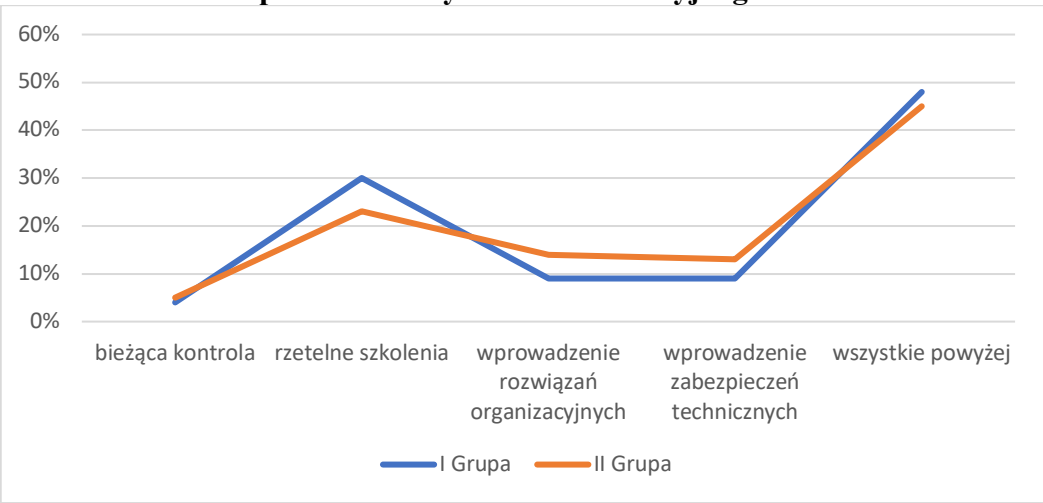
Tabela 4-21
Procentowy rozkład odpowiedzi dotyczący elementów bezpieczeństwa systemu informacyjnego PSP.

Odpowiedzi	I Grupa PRACOWNICY KW		II Grupa PRACOWNICY KM/KP		Ogółem	
	Struktura liczbowa	Struktura procentowa (%)	Struktura liczbowa	Struktura procentowa (%)	Struktura liczbowa	Struktura procentowa (%)
bieżąca kontrola i nadzór	13	4	70	5	83	4
rzetelne szkolenia dla funkcjonariuszy i pracowników	107	30	356	23	463	24
wprowadzenie właściwych rozwiązań organizacyjnych	31	9	216	14	247	13
wprowadzenie właściwych zabezpieczeń technicznych	32	9	207	13	239	13
wszystkie powyżej	169	48	696	45	865	46
Ogółem	352	100	1545	100	1897	100

Źródło: Opracowanie własne.

W celu dokładniejszego zobrazowania uzyskanych rozkładów udzielonych odpowiedzi z obu grup, wyniki zaprezentowano na wykresie 4-22.

Wykres 4-22
Procentowy rozkład odpowiedzi w obu grupach badawczych dotyczący elementów bezpieczeństwa systemu informacyjnego PSP.



Zaprezentowany, powyższy wykres wskazuje na nieduże rozbieżności, które wynikają z udzielonych przez wszystkich ankietowanych odpowiedzi. W celu zbadania tejże istotności wykonano test współczynnika korelacji liniowej r- Pearsona.

Tabela 4-22
Rozkład odpowiedzi dotyczący elementów bezpieczeństwa systemu informacyjnego PSP.

Odpowiedzi	I Grupa KW	II Grupa KM/KP	Ogółem		
	x_i	y_i	x_i^2	y_i^2	$x_i * y_i$
bieżąca kontrola i nadzór	13	70	169	4900	910
rzetelne szkolenia dla funkcjonariuszy i pracowników	107	356	11449	126736	38092
wprowadzenie właściwych rozwiązań organizacyjnych	31	216	961	46656	6696
wprowadzenie właściwych zabezpieczeń technicznych	32	207	1024	42849	6624
wszystkie powyżej	169	696	28561	484416	117624
Ogółem	$\sum_{i=5}^{n} x_i =$ 352	$\sum_{i=5}^{n} y_i =$ 1545	$\sum_{i=5}^{n} x_i^2 =$ 42164	$\sum_{i=5}^{n} y_i^2 =$ 705557	$\sum_{i=5}^{n} x_i * y_i =$ 169946
$\bar{x} = \frac{1}{n}\sum_{i=n}^{n} x_i = \frac{1}{5} * 352 \approx 70$ $x^2 = 4900$ $\bar{y} = \frac{1}{n}\sum_{i=n}^{n} y_i = \frac{1}{5} * 1545 = 309$ $y^2 = 95\,481$					

Źródło: Opracowanie własne.

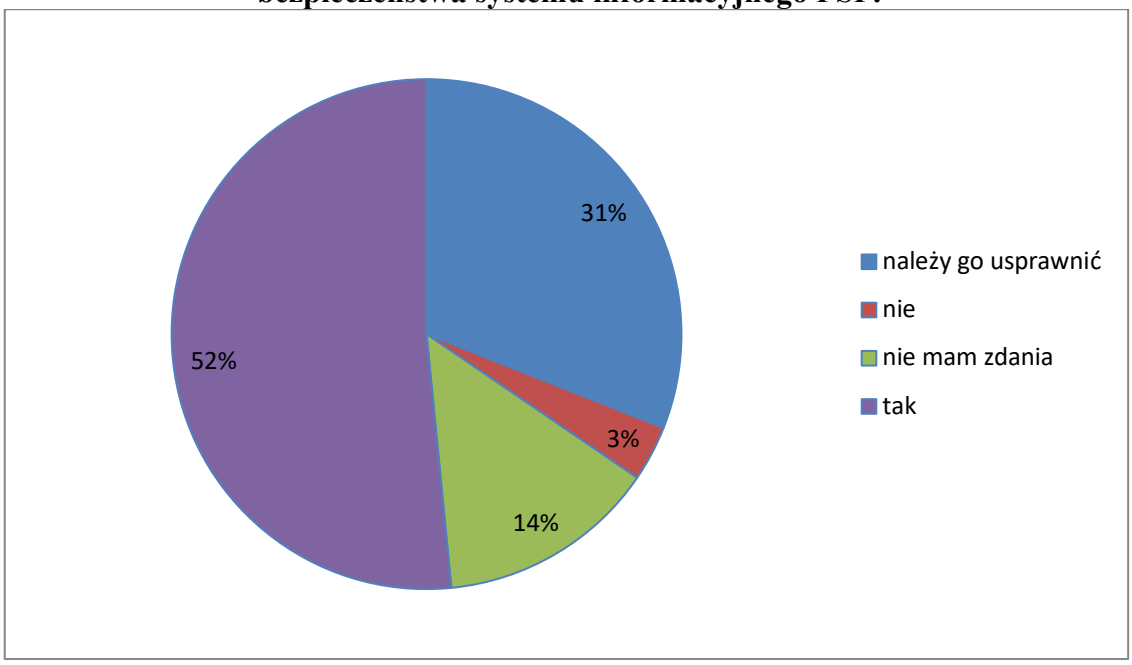
$$r = \frac{\frac{1}{n}\sum_{i=n}^{n} x_i y_i - xy}{\sqrt{(\frac{1}{n}\sum_{i=n}^{n} x_i^2 - x^2)(\frac{1}{n}\sum_{i=n}^{n} y_i^2 - y^2)}} = \frac{\frac{1}{5} * 169946 - 21\,630}{\sqrt{(\frac{1}{5} * 42164 - 4900)(\frac{1}{5} * 705557 - 95481)}} \approx 0{,}97$$

Przedstawiona powyższa analiza ukazuje, że współczynnik korelacji liniowej Pearsona wynosi r ≈ 0,97, co wskazuje na korelacje dodatnią o bardzo silnej zależności. Świadczy to o tym, iż wzrost wartości w udzielonych odpowiedziach jednej z grup powoduje wzrost wartości odpowiedzi drugiej z grup.

W ramach przeprowadzonych badań empirycznych poproszono respondentów o udzielenie odpowiedzi na pytanie dwunaste (zał. 1): 12. *Czy przyjęty w Pani/Pana macierzystej jednostce system obiegu informacji spełnia oczekiwania funkcjonalne?*

W tym pytaniu badanym zaproponowano cztery warianty odpowiedzi, jednokrotnego wyboru. Ogólny rozkład odpowiedzi został zaprezentowany na wykresie 4-23, z którego wynika, iż najwięcej opiniodawców odpowiedziało się za wariantem, iż przyjęty w jednostce obieg informacji spełnia oczekiwania użytkowników, o czym świadczy 52 % uzyskanych odpowiedzi, na co złożyło się 978 wskazań. Następną z kolei wskazywaną odpowiedzią było, że system trzeba usprawnić 31 % (588 wskazań). 14 % ankietowanych nie miało zdania w tym temacie (264 wskazania), natomiast negatywnie oceniło system 3 % próby badawczej (67 wskazań).

Wykres 4-23
Procentowy rozkład odpowiedzi w obu grupach badawczych dotyczący elementów bezpieczeństwa systemu informacyjnego PSP.



Źródło: Opracowanie własne.

Respondenci należący do I grupy najczęściej wskazywali na odpowiedź, że przyjęty w jednostce obieg informacji spełnia oczekiwania użytkowników – odpowiedź ta uzyskała 49 %, co stanowiło 174 wskazania. Na drugim miejscu uplasował się wariant odpowiedzi, że system należy usprawnić, wskazania takiego dokonało 119 respondentów – 34 %. Trzecim wariantem została odpowiedź, w której badani tej grupy nie mieli zadania w tym temacie, na którą zdecydowało się 44 ankietowanych - 13 %. Negatywnie system obiegu informacji oceniło 4 % ankietowanych, na co złożyło się 15 wskazań.

W II grupie ankietowanych odpowiedzi rozłożyły się całkiem podobnie. Zdecydowana większość respondentów wybrała wariant odpowiedzi, iż przyjęty w jednostce obieg informacji spełnia oczekiwania użytkowników 804 wskazań – 52 %. Wariant odpowiedzi

o konieczności usprawnienia systemu wybrało 469 respondentów – 30 %. Natomiast trzecim wyborem w tej grupie została odpowiedź nie mam zdania, na którą zdecydowało się 220 ankietowanych - 14 %. Podobnie jak w pierwszej grupie najrzadziej wybieraną odpowiedzią wśród ankietowanych była ta dotyczącą negatywnej oceny systemy w zakresie funkcjonalnym, którą wybrało tylko 52 osoby - 4 %.

Szczegółowy rozkład danych odpowiedzi został ukazany w tabeli 4-23.

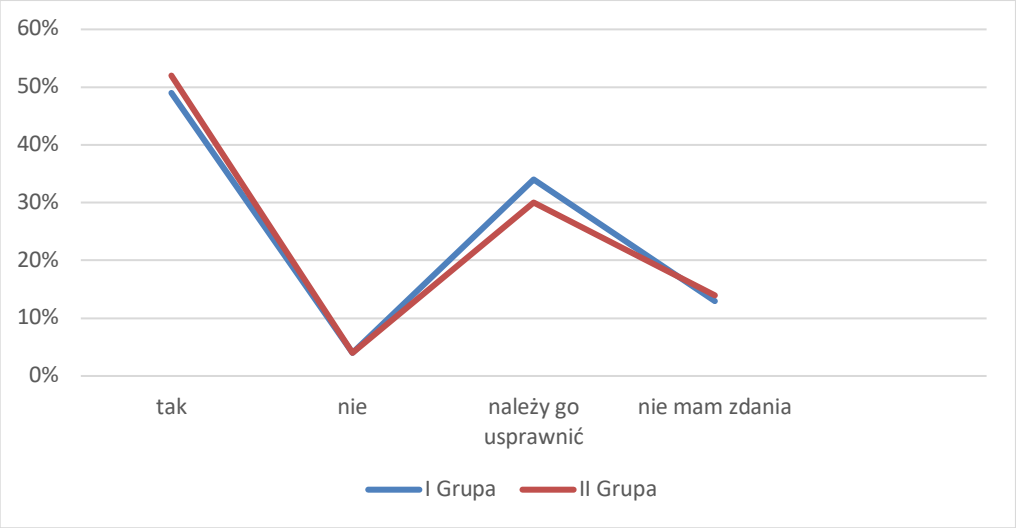
Tabela 4-23
Procentowy rozkład odpowiedzi dotyczący spełnienia oczekiwań funkcjonalnych przez system obiegu informacji.

Odpowiedzi	I Grupa PRACOWNICY KW		II Grupa PRACOWNICY KM/KP		Ogółem	
	Struktura liczbowa	Struktura procentowa (%)	Struktura liczbowa	Struktura procentowa (%)	Struktura liczbowa	Struktura procentowa (%)
należy go usprawnić	119	34	469	30	588	31
Nie	15	4	52	4	67	3
nie mam zdania	44	13	220	14	264	14
Tak	174	49	804	52	978	52
Ogółem	352	100	1545	100	1897	100

Źródło: Opracowanie własne.

W celu dokładniejszego zobrazowania uzyskanych rozkładów udzielonych odpowiedzi z obu grup, wyniki zaprezentowano na wykresie 4-24.

Wykres 4-24
Procentowy rozkład odpowiedzi w obu grupach badawczych dotyczący spełnienia oczekiwań funkcjonalnych przez system obiegu informacji.



Zaprezentowany, powyższy wykres wskazuje na minimalne rozbieżności, które wynikają z udzielonych przez wszystkich ankietowanych odpowiedzi. W celu zbadania tejże istotności wykonano test współczynnika korelacji liniowej r- Pearsona.

Tabela 4-24
Rozkład odpowiedzi dotyczący spełnienia oczekiwań funkcjonalnych przez system obiegu informacji.

Odpowiedzi	I Grupa KW	II Grupa KM/KP	Ogółem		
	x_i	y_i	x_i^2	y_i^2	$x_i * y_i$
należy go usprawnić	119	469	14161	219961	55811
nie	15	52	225	2704	780
nie mam zdania	44	220	1936	48400	9680
tak	174	804	30276	646416	139896
Ogółem	$\sum_{i=3}^{n} x_i =$ 352	$\sum_{i=3}^{n} y_i =$ 1545	$\sum_{i=3}^{n} x_i^2 =$ 46598	$\sum_{i=3}^{n} y_i^2 =$ 917481	$\sum_{i=3}^{n} x_i * y_i =$ 206167
$\bar{x} = \frac{1}{n}\sum_{i=n}^{n} x_i = \frac{1}{4} * 352 \approx 88$ $x^2 \approx 7\,744$ | $\bar{y} = \frac{1}{n}\sum_{i=n}^{n} y_i = \frac{1}{4} * 1545 \approx 386$ $y^2 \approx 148\,996$					

Źródło: Opracowanie własne.

$$r = \frac{\frac{1}{n}\sum_{i=n}^{n} x_i y_i - xy}{\sqrt{(\frac{1}{n}\sum_{i=n}^{n} x_i^2 - x^2)(\frac{1}{n}\sum_{i=n}^{n} y_i^2 - y^2)}} = \frac{\frac{1}{4} * 206167 - 33\,968}{\sqrt{(\frac{1}{4} * 46598 - 7\,744)(\frac{1}{4} * 917481 - 148\,996)}} \approx 0{,}99$$

Obliczony współczynnik wynosi w przybliżeniu r = 0,99 i należy stwierdzić, iż jest to korelacja dodatnia o bardzo wysokim charakterze. Świadczy to o występującej dość silnej zależności pomiędzy przynależnością do grupy, a wskazywaniem danej odpowiedzi oraz oznacza to, iż wzrost wartości odpowiedzi jednej z grup wpływa na wzrost wartości odpowiedzi drugiej z grup.

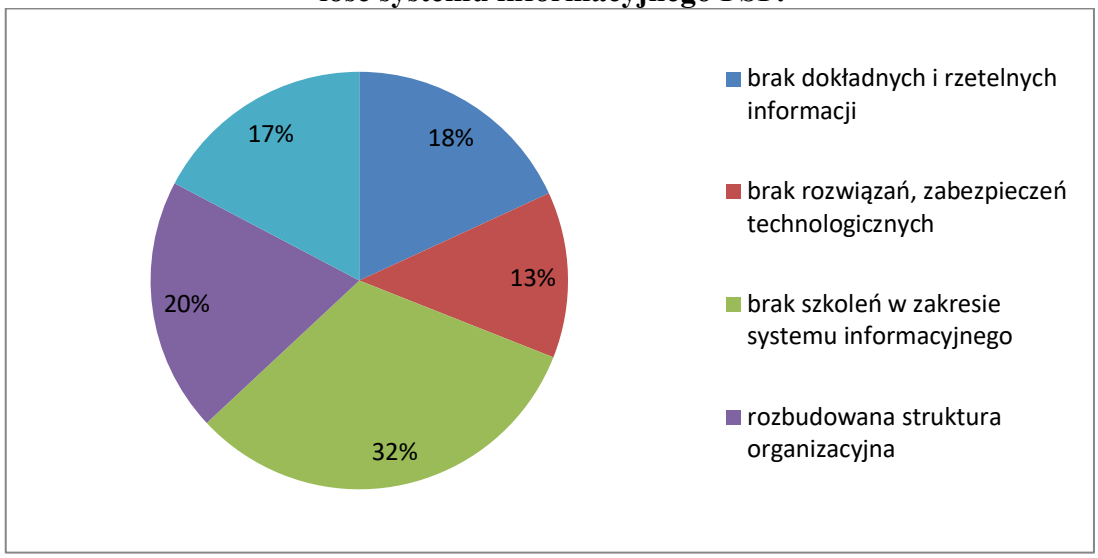
W ramach przeprowadzonych badań empirycznych poproszono respondentów o udzielenie odpowiedzi na kolejne trzynaste pytanie (zał. 1): 13. *Który z przedstawionych poniżej czynników Pani/Pana zdaniem wpływa najbardziej na niedoskonałość systemu informacyjnego w PSP?*

Respondenci mieli do wyboru jedną możliwą odpowiedź spośród pięciu zaproponowanych wariantów: brak dokładnych i rzetelnych informacji; brak rozwiązań, zabezpieczeń technologicznych; brak szkoleń w zakresie systemu informacyjnego; rozbudowana struktura organizacyjna, system informacyjny jest sprawny i nie potrzebuje ulepszeń. Ogólny rozkład odpowiedzi został zilustrowany na wykresie 4-25, z analizy którego wynika, iż wśród wszystkich ankietowanych najczęściej wybierana była odpowiedź, że za nie-

doskonałość systemu informacyjnego w PSP najbardziej odpowiada brak szkoleń w zakresie systemu informacyjnego, czego dowodem jest uzyskana liczba 608 wskazań na tą odpowiedź na poziomie 32 %. Kolejne odpowiedzi uzyskały stosunkowo mniejsze, choć wyrównane wyniki. Na drugim miejscu wśród odpowiedzi respondenci wskazali rozbudowaną struktura organizacyjna 20 % (373 wskazań), potem brak dokładnych i rzetelnych informacji 18 % (350 wskazań), system informacyjny jest sprawny i nie potrzebuje ulepszeń 17 % (322 wskazań). Najmniej liczna część respondentów wskazała na odpowiedź brak rozwiązań, zabezpieczeń technologicznych 13 % głosów (244 wskazań).

Szczegółowy rozkład odpowiedzi został zilustrowany w tabeli 4-25.

Wykres 4-25
Procentowy rozkład odpowiedzi dotyczący czynników wpływających na niedoskonałość systemu informacyjnego PSP.



Źródło: Opracowanie własne.

Badani należący do I grupy najczęściej wskazywali na wariant odpowiedzi mówiący, że za niedoskonałość systemu informacyjnego w PSP najbardziej odpowiada brak szkoleń w zakresie systemu informacyjnego, o czym świadczy 32 % i 111 wskazań. Na drugim miejscu wskazywano brak dokładnych i rzetelnych informacji 22% i 79 wskazań. Następnie równorzędnie dwie odpowiedzi uzyskały ten sam wynik, a mianowicie: system informacyjny jest sprawny i nie potrzebuje ulepszeń oraz rozbudowana struktura organizacyjna po 19 % - 67 wskazań. Na ostatnim miejscu respondenci wskazywali, brak rozwiązań, zabezpieczeń technologicznych 8 % i 27 wskazań.

W II grupie respondentów odpowiedzi rozłożyły się następująco. Pierwszą odpowiedzią, analogicznie do pierwszej grupy, była brak szkoleń w zakresie systemu informacyjnego 32 % (497 wskazań). Następnie rozbudowana struktura organizacyjna 20 % - 306 wskazań i kolejno brak dokładnych i rzetelnych informacji 18 % - 271 wskazań; system

informacyjny jest sprawny i nie potrzebuje ulepszeń 16 % - 255 wskazań;. Natomiast odpowiedź brak rozwiązań, zabezpieczeń technologicznych uzyskała 216 wskazań, co daje 14 % całości odpowiedzi.

Szczegółowy rozkład odpowiedzi dotyczący występujących zagrożeń zaprezentowano w tabeli 4.

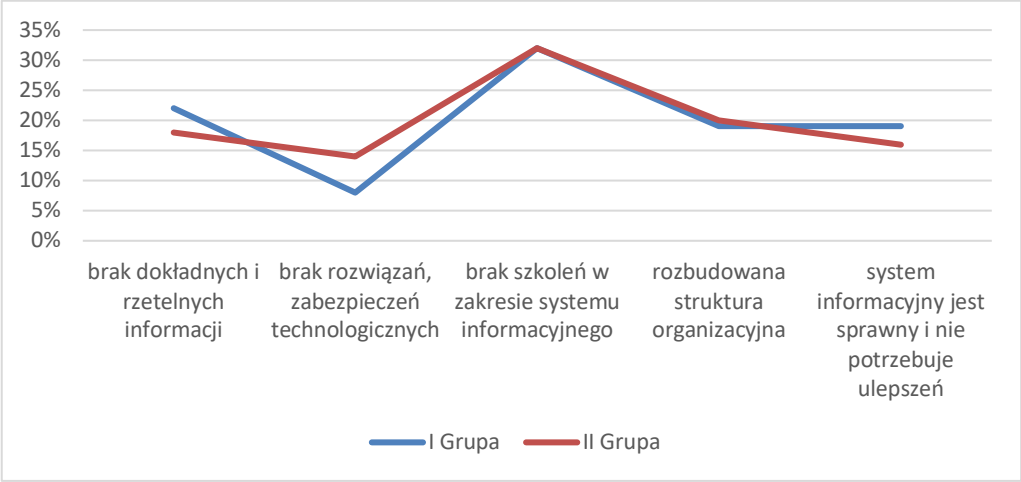
Tabela 4-25
Procentowy rozkład odpowiedzi dotyczący czynników wpływających na niedoskonałość systemu informacyjnego PSP.

Odpowiedzi	I Grupa PRACOWNICY KW		II Grupa PRACOWNICY KM/KP		Ogółem	
	Struktura liczbowa	Struktura procentowa (%)	Struktura liczbowa	Struktura procentowa (%)	Struktura liczbowa	Struktura procentowa (%)
brak dokładnych i rzetelnych informacji	79	22	271	18	350	18
brak rozwiązań, zabezpieczeń technologicznych	27	8	216	14	244	17
brak szkoleń w zakresie systemu informacyjnego	111	32	497	32	608	32
rozbudowana struktura organizacyjna	67	19	306	20	373	20
system informacyjny jest sprawny i nie potrzebuje ulepszeń	67	19	255	16	322	113
Ogółem	352	100	1545	100	1897	100

Źródło: Opracowanie własne.

W celu dokładniejszego zobrazowania uzyskanych rozkładów udzielonych odpowiedzi z obu grup, wyniki zaprezentowano na wykresie 4-26.

Wykres 4-26
Procentowy rozkład odpowiedzi w obu grupach badawczych dotyczący czynników wpływających na niedoskonałość systemu informacyjnego PSP.



Zaprezentowany, powyższy wykres wskazuje na niewielkie rozbieżności, które wynikają z udzielonych przez wszystkich ankietowanych odpowiedzi. W celu zbadania tejże istotności wykonano test współczynnika korelacji liniowej r- Pearsona.

Tabela 4-26
Rozkład odpowiedzi dotyczący czynników wpływających na niedoskonałość systemu informacyjnego PSP.

Odpowiedzi	I Grupa KW	II Grupa KM/KP	Ogółem		
	x_i	y_i	x_i^2	y_i^2	$x_i * y_i$
brak dokładnych i rzetelnych informacji	79	271	6241	73441	21409
brak rozwiązań, zabezpieczeń technologicznych	27	216	729	46656	5832
brak szkoleń w zakresie systemu informacyjnego	111	497	12321	247009	55167
rozbudowana struktura organizacyjna	67	306	4489	93636	20502
system informacyjny jest sprawny i nie potrzebuje ulepszeń	67	255	4489	65025	17085
Ogółem	$\sum_{i=5}^{n} x_i =$ 352	$\sum_{i=5}^{n} y_i =$ 1545	$\sum_{i=5}^{n} x_i^2 =$ 28269	$\sum_{i=5}^{n} y_i^2 =$ 525767	$\sum_{i=5}^{n} x_i * y_i =$ 119995
$\bar{x} = \frac{1}{n}\sum_{i=n}^{n} x_i = \frac{1}{5} * 352 \approx 70$ $x^2 = 4900$ $\bar{y} = \frac{1}{n}\sum_{i=n}^{n} y_i = \frac{1}{5} * 1545 = 309$ $y^2 = 95\,481$					

Źródło: Opracowanie własne.

$$r = \frac{\frac{1}{n}\sum_{i=n}^{n} x_i y_i - xy}{\sqrt{(\frac{1}{n}\sum_{i=n}^{n} x_i^2 - x^2)(\frac{1}{n}\sum_{i=n}^{n} y_i^2 - y^2)}} = \frac{\frac{1}{5} * 119995 - 21\,630}{\sqrt{(\frac{1}{5} * 28269 - 4900)(\frac{1}{5} * 525767 - 95481)}} \approx 0{,}87$$

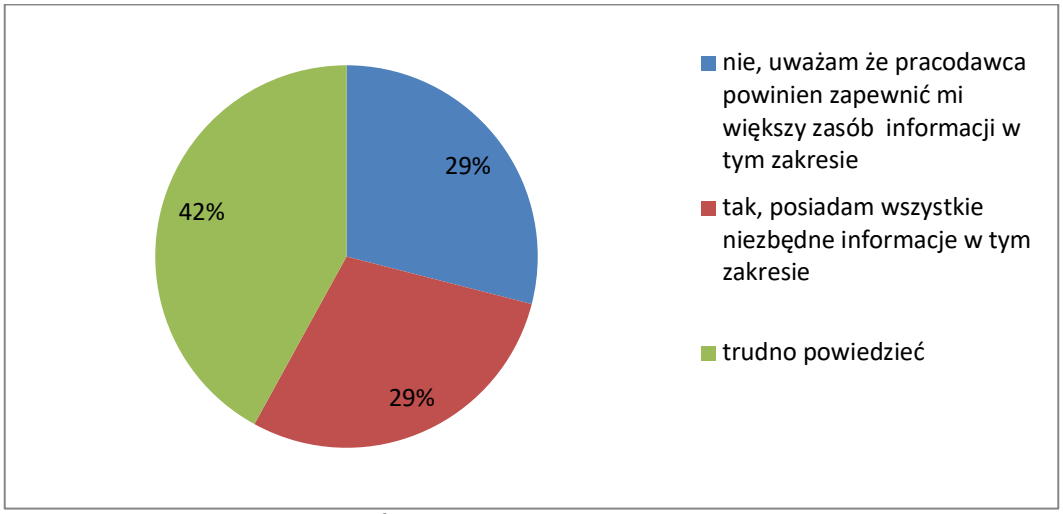
Obliczony współczynnik wynosi w przybliżeniu 0,84. Można stwierdzić, iż jest to korelacja dodatnia o bardzo wysokim charakterze. Świadczy to o występującej dość silnej zależności pomiędzy przynależnością do grupy a wskazywaniem odpowiedzi. Oznacza to, iż wzrost wartości odpowiedzi jednej z grup wpływa na wzrost wartości odpowiedzi drugiej z grup.

W ramach przeprowadzonych badań empirycznych poproszono respondentów o udzielenie odpowiedzi na pytanie czternaste (zał. 1): 14. *Czy Pani/Pana zdaniem funkcjonujący w jednostce system szkoleń w zakresie systemu informacyjnego i jego bezpieczeństwa jest właściwy?*

Badanym zaproponowano trzy warianty odpowiedzi, jednokrotnego wyboru, w wyniku czego uzyskano 1897 wskazań: tak, posiadam wszystkie niezbędne informacje w tym zakresie; nie, uważam że pracodawca powinien zapewnić mi większy zasób informacji w tym zakresie oraz ostatni wariant trudno powiedzieć. Ogólny rozkład odpowiedzi został zaprezentowany na wykresie 4-27, z którego wynika, iż najwięcej opiniodawców odpowiedziało się za wariantem, trudno powiedzieć, o czym świadczy 42 % uzyskanych odpowiedzi, na co złożyło się 820 wskazań. Kolejne dwa warianty odpowiedzi uzyskały praktycznie identyczne wyniki, a mianowicie: nie, uważam że pracodawca powinien zapewnić mi większy zasób informacji w tym zakresie – 29 % (547 wskazań); tak, posiadam wszystkie niezbędne informacje w tym zakresie – 29 % próby badawczej (546 wskazań).

Szczegółowy rozkład został ujęty w tabeli 4-27.

Wykres 4-27
Procentowy rozkład odpowiedzi dotyczący prawidłowości szkoleń w zakresie bezpieczeństwa informacji.



Źródło: Opracowanie własne.

Respondenci należący do I grupy w tym pytaniu najczęściej wskazywali na odpowiedź trudno powiedzieć – odpowiedź ta uzyskała 41 %, co stanowiło 145 wskazania. Na drugim miejscu uplasował się wariant odpowiedzi nie, uważam że pracodawca powinien zapewnić mi większy zasób informacji w tym zakresie, gdzie wskazania takiego dokonały 111 osoby, co dało wynik 32 % respondentów. Natomiast na wariant odpowiedzi tak, posiadam wszystkie niezbędne informacje w tym zakresie 27 % ankietowanych z liczbą 96 wskazań.

Trochę inaczej ukształtował się układ procentowy odpowiedzi udzielonych przez respondentów II grupy. Podobnie jak w I grupie najwięcej odpowiedzi otrzymała odpowiedź trudno powiedzieć, o czym świadczy 44 %, czyli 675 wskazań. Następnie 29 % uzyskał wariant odpowiedzi: tak, posiadam wszystkie niezbędne informacje w tym zakresie z liczbą 442 wskazań. Wariant z odpowiedzią nie, uważam że pracodawca powinien zapewnić mi większy zasób informacji w tym zakresie uplasował się na trzecim miejscu z wynikiem 27 %, na co złożyły się 428 wskazania.

Szczegółowy rozkład danych odpowiedzi został ukazany w tabeli 4-27.

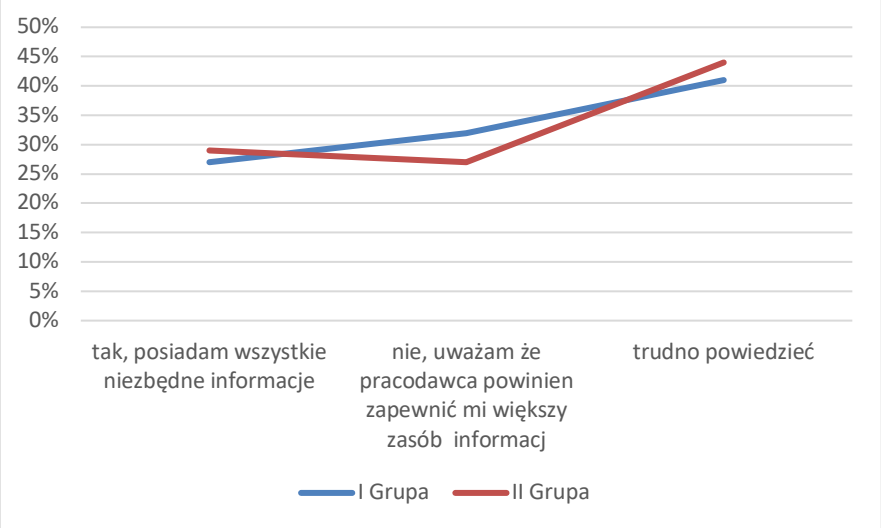
Tabela 4-27
Procentowy rozkład odpowiedzi dotyczący prawidłowości szkoleń w zakresie bezpieczeństwa informacji.

Odpowiedzi	I Grupa PRACOWNICY KW		II Grupa PRACOWNICY KM/KP		Ogółem	
	Struktura liczbowa	Struktura procentowa (%)	Struktura liczbowa	Struktura procentowa (%)	Struktura liczbowa	Struktura procentowa (%)
tak, posiadam wszystkie niezbędne informacje w tym zakresie	96	27	442	29	546	28
nie, uważam że pracodawca powinien zapewnić mi większy zasób informacji w tym zakresie	111	32	428	27	547	29
trudno powiedzieć	145	41	675	44	820	43
Ogółem	352	100	1545	100	1897	100

Źródło: Opracowanie własne.

W celu dokładniejszego zobrazowania uzyskanych rozkładów udzielonych odpowiedzi z obu grup, wyniki zaprezentowano na wykresie 4-28.

Wykres 4-28
Procentowy rozkład odpowiedzi w obu grupach badawczych dotyczący prawidłowości szkoleń w zakresie bezpieczeństwa informacji.



Zaprezentowany, powyższy wykres wskazuje na niewielkie rozbieżności, które wynikają z udzielonych przez wszystkich ankietowanych odpowiedzi. W celu zbadania tejże istotności wykonano test współczynnika korelacji liniowej r- Pearsona.

Tabela 4-28
Rozkład odpowiedzi dotyczący prawidłowości szkoleń w zakresie bezpieczeństwa informacji.

Odpowiedzi	I Grupa KW	II Grupa KM/KP	Ogółem		
	x_i	y_i	x_i^2	y_i^2	$x_i * y_i$
Tak	96	442	9216	195364	42432
Nie	111	428	12321	183184	47508
trudno powiedzieć	145	675	21025	455625	97875
Ogółem	$\sum_{i=3}^{n} x_i$= 352	$\sum_{i=3}^{n} y_i$= 1545	$\sum_{i=3}^{n} x_i^2$ = 42562	$\sum_{i=3}^{n} y_i^2$ = 834173	$\sum_{i=3}^{n} x_i * y_i$ = 187815
$\bar{x} = \frac{1}{n}\sum_{i=n}^{n} x_i = \frac{1}{3} * 352 \approx 117$ $x^2 \approx 13689$ | $\bar{y} = \frac{1}{n}\sum_{i=n}^{n} y_i = \frac{1}{3} * 1545 \approx 509$ $y^2 \approx 259\,081$					

Źródło: Opracowanie własne.

$$r = \frac{\frac{1}{n}\sum_{i=n}^{n} x_i y_i - xy}{\sqrt{(\frac{1}{n}\sum_{i=n}^{n} x_i^2 - x^2)(\frac{1}{n}\sum_{i=n}^{n} y_i^2 - y^2)}} = \frac{\frac{1}{3} * 187815 - 59044}{\sqrt{(\frac{1}{3} * 42562 - 13689)(\frac{1}{3} * 834173 - 259081)}} \approx 0{,}93$$

Po przeprowadzeniu testu współczynnika korelacji liniowej r- Pearsona, otrzymano wynik r ≈ 0,93, co świadczy, że pomiędzy poszczególnymi grupami występuje bardzo silna zależność i mówimy o korelacji dodatniej. Oznacza to, iż wzrost wartości odpowiedzi jednej z grup wpływa na wzrost wartości odpowiedzi drugiej z grup.

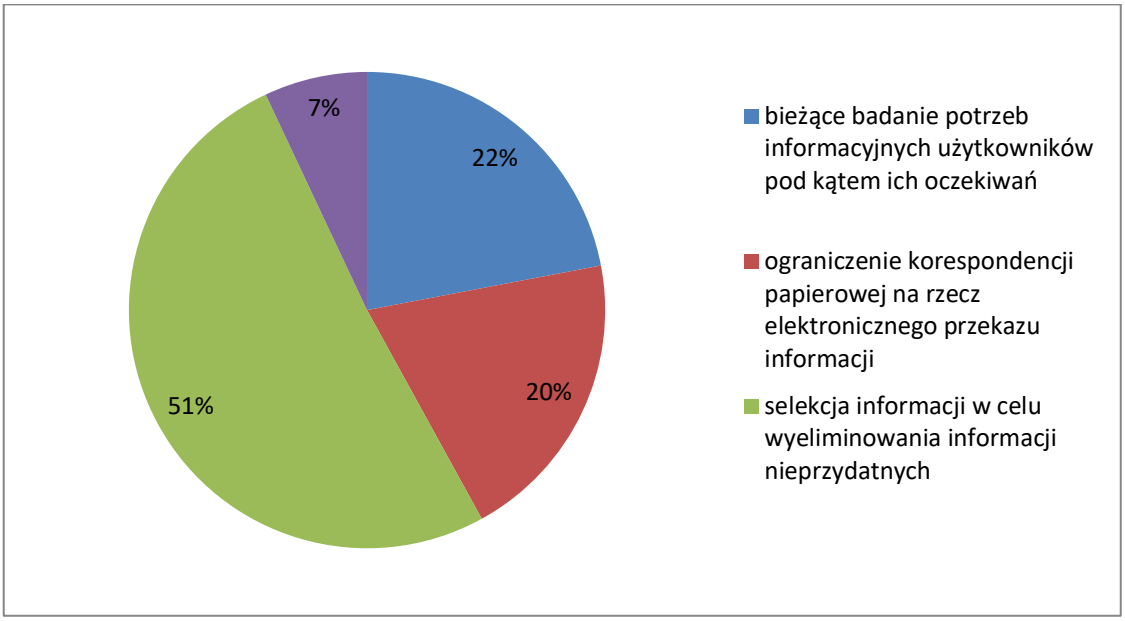
W ramach przeprowadzonych badań empirycznych poproszono respondentów o udzielenie odpowiedzi na pytanie pietnaste (zał. 1): 15. *Które z poniższych działań Pani/Pana zadaniem mogą poprawić skuteczność funkcjonowania systemu informacyjnego w PSP?*

Badanym zaproponowano cztery warianty odpowiedzi, jednokrotnego wyboru. Ogólny rozkład odpowiedzi został zaprezentowany na wykresie 4-29, z którego wynika, iż najwięcej opiniodawców odpowiedziało się za wariantem odpowiedzi, że to selekcja informacji w celu wyeliminowania informacji nieprzydatnych może mieć największy wpływ na funkcjonowanie systemu 51 % z 976 wskazaniami. Następnie wskazywano, iż bieżące badanie potrzeb informacyjnych użytkowników pod kątem ich oczekiwań 22 % z 424 wskazaniami, kolejno uplasowała się odpowiedź o ograniczeniu korespondencji papiero-

wej na rzecz elektronicznego przekazu 20 % z 373 wskazaniami i na końcu o spłaszczeniu struktury organizacyjnej jednostki 7 % z 124 wskazaniami.

Szczegółowy rozkład został ujęty w tabeli 4-29.

Wykres 4-29
Procentowy rozkład odpowiedzi dotyczący działań mogących poprawić skuteczność funkcjonowania systemu informacyjnego w PSP.



Źródło: Opracowanie własne.

W rozbiciu na poszczególne grupy respondentów odpowiedzi kształtowały się następująco. Ankietowani należący do I grupy najczęściej wskazywali na odpowiedź, selekcja informacji w celu wyeliminowania informacji nieprzydatnych - odpowiedź ta uzyskała 41 %, co stanowiło 144 wskazania. Na drugim miejscu uplasował się wariant odpowiedzi, bieżące badanie potrzeb informacyjnych użytkowników pod kątem ich oczekiwań, gdzie wskazania takiego dokonało 95 respondentów – 27 %. Trzecim wariantem została odpowiedź, ograniczenie korespondencji papierowej na rzecz elektronicznego przekazu informacji, na którą zdecydowało się 89 ankietowanych - 25 %. Na ostatnim miejscu ankietowani wskazali, spłaszczenie struktury organizacyjnej jednostki 24 wskazania, co daje 7 % całości odpowiedzi.

W II grupie ankietowanych odpowiedzi były zbieżne z odpowiedziami w I grupie. Największa część respondentów zdecydowała się na odpowiedź, selekcja informacji w celu wyeliminowania informacji nieprzydatnych, 832 wskazań – 54 %. Wariant odpowiedzi, bieżące badanie potrzeb informacyjnych użytkowników pod kątem ich oczekiwań

wybrało 329 respondentów – 21 %. Natomiast trzecim wyborem w tej grupie została odpowiedź ograniczenie korespondencji papierowej na rzecz elektronicznego przekazu informacji, na którą zdecydowało się 284 ankietowanych - 18 %. Najrzadziej wybieraną odpowiedzią wśród ankietowanych dotyczącą tego pytania była odpowiedź spłaszczenie struktury organizacyjnej jednostki, którą wybrało 100 osób - 7 %.

Szczegółowy rozkład danych odpowiedzi został ukazany w tabeli 4-29.

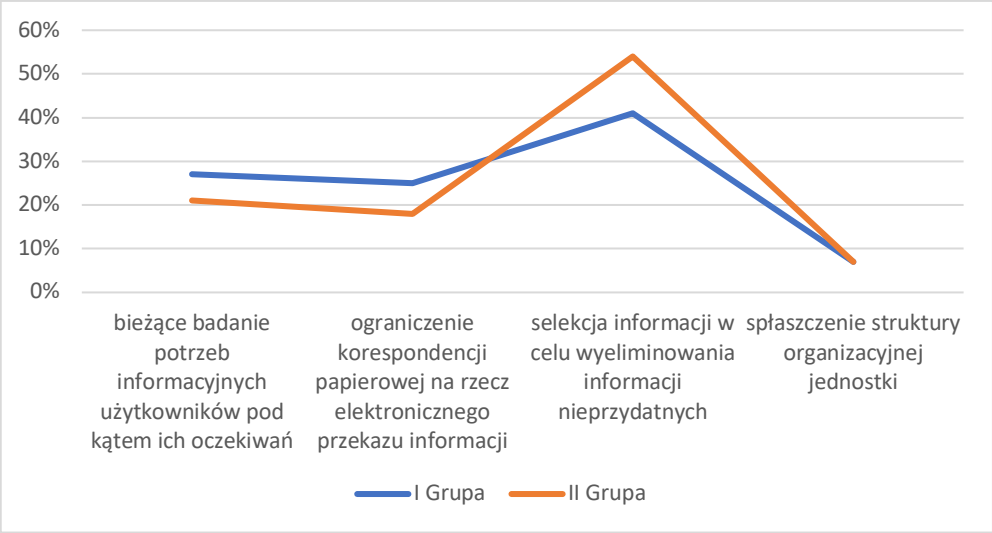
Tabela 4-29
Procentowy rozkład odpowiedzi dotyczący działań mogących poprawić skuteczność funkcjonowania systemu informacyjnego w PSP.

Odpowiedzi	I Grupa PRACOWNICY KW		II Grupa PRACOWNICY KM/KP		Ogółem	
	Struktura liczbowa	Struktura procentowa (%)	Struktura liczbowa	Struktura procentowa (%)	Struktura liczbowa	Struktura procentowa (%)
bieżące badanie potrzeb informacyjnych użytkowników pod kątem ich oczekiwań	95	27	329	21	424	22
ograniczenie korespondencji papierowej na rzecz elektronicznego przekazu informacji	89	25	284	18	373	20
selekcja informacji w celu wyeliminowania informacji nieprzydatnych	144	41	832	54	976	51
spłaszczenie struktury organizacyjnej jednostki	24	7	100	7	124	7
Ogółem	352	100	1545	100	1897	100

Źródło: Opracowanie własne.

W celu dokładniejszego zobrazowania uzyskanych rozkładów udzielonych odpowiedzi z obu grup, wyniki zaprezentowano na wykresie 4-30.

Wykres 4-30
Procentowy rozkład odpowiedzi w obu grupach badawczych dotyczący działań mogących poprawić skuteczność funkcjonowania systemu informacyjnego w PSP.



Zaprezentowany, powyższy wykres wskazuje na rozbieżności, które wynikają z udzielonych przez wszystkich ankietowanych odpowiedzi. W celu zbadania tejże istotności wykonano test współczynnika korelacji liniowej r- Pearsona.

Tabela 4-30
Rozkład odpowiedzi dotyczący działań mogących poprawić skuteczność funkcjonowania systemu informacyjnego w PSP.

Odpowiedzi	**I Grupa KW**	**II Grupa KM/KP**	**Ogółem**		
	x_i	y_i	x_i^2	y_i^2	$x_i * y_i$
informacje są często niezrozumiałe	95	329	9025	108241	31255
przełożeni wymagają zbyt wiele	89	284	7921	80656	25276
wiadomości zawierają zbyt wiele danych	144	832	20736	692224	119808
komunikaty są za oficjalne	24	100	576	10000	2400
Ogółem	$\sum_{i=3}^{n} x_i =$ 352	$\sum_{i=3}^{n} y_i =$ 1545	$\sum_{i=3}^{n} x_i^2 =$ 38258	$\sum_{i=3}^{n} y_i^2 =$ 891121	$\sum_{i=3}^{n} x_i * y_i =$ 178739
$\bar{x} = \frac{1}{n}\sum_{i=n}^{n} x_i = \frac{1}{4} * 352 \approx 88$ $x^2 \approx 7\,744$ | $\bar{y} = \frac{1}{n}\sum_{i=n}^{n} y_i = \frac{1}{4} * 1545 \approx 386$ $y^2 \approx 148\,996$					

Źródło: Opracowanie własne.

$$r = \frac{\frac{1}{n}\sum_{i=n}^{n} x_i y_i - xy}{\sqrt{(\frac{1}{n}\sum_{i=n}^{n} x_i^2 - x^2)(\frac{1}{n}\sum_{i=n}^{n} y_i^2 - y^2)}} = \frac{\frac{1}{4} * 178739 - 33\,968}{\sqrt{(\frac{1}{4} * 38258 - 7\,744\,)(\frac{1}{4} * 8911215 - 148\,996)}} \approx 0{,}92$$

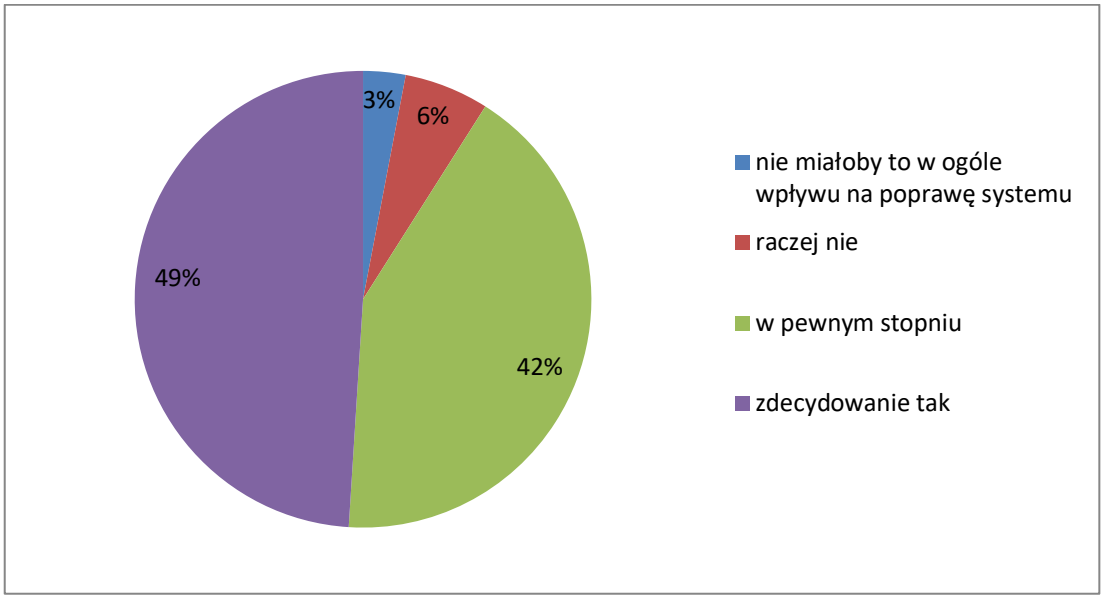
Obliczony współczynnik wynosi w przybliżeniu r ≈ 0,92. Można stwierdzić, iż jest to korelacja dodatnia o bardzo wysokim charakterze. Świadczy to o występującej dość silnej zależności pomiędzy przynależnością do grupy, a wskazywaniem odpowiedzi. Oznacza to, iż wzrost wartości odpowiedzi jednej z grup wpływa na wzrost wartości odpowiedzi drugiej z grup.

W ramach przeprowadzonych badań empirycznych poproszono opiniodawców o udzielenie odpowiedzi na kolejne pytanie szesnaste (zał. 1): 16. *Czy według Pana/Pani pełne ujednolicenie systemów teleinformatycznych na wszystkich poziomach organizacyjnych PSP zwiększyłoby efektywność bezpieczeństwa systemu informacyjnego?*

Respondenci mogli wybrać zaledwie jedną możliwość spośród czterech zaproponowanych wariantów, a dokładniej: nie miałoby to w ogóle wpływu na poprawę systemu, raczej nie, w pewnym stopniu, zdecydowanie tak. Ogólny rozkład odpowiedzi został zilustrowany na wykresie 4-31, z analizy którego wynika, iż odpowiedź zdecydowanie tak była najczęściej wybieraną odpowiedzią wśród wszystkich respondentów biorących udział w badaniu, czego dowodem jest uzyskana liczba wskazań na tą odpowiedź na poziomie 49 % (923 wskazań). Na drugim miejscu wśród odpowiedzi respondenci wskazali odpowiedź w pewnym stopniu, która uzyskała 42 %, na co złożyło się odpowiednio 800 wskazań. Kolejna część respondentów wskazała na odpowiedź raczej nie, na co złożyło się uzyskanie 6 % poparcia (127 wskazań) i na ostatnim miejscu wybierano odpowiedź nie miałoby to w ogóle wpływu na poprawę systemu z 47 wskazaniami i 3 % wyborów.

Szczegółowy rozkład odpowiedzi został zilustrowany w tabeli 4-31.

Wykres 4-31
Procentowy rozkład odpowiedzi dotyczący wpływu ujednolicenia systemów teleinformatycznych PSP na bezpieczeństwo systemu informacyjnego.



Źródło: Opracowanie własne.

Badani należący do I grupy najczęściej wskazywali na wariant odpowiedzi zdecydowanie tak o czym świadczy 193 wskazania i wynik 55 %. Mniej wskazań otrzymała kolejna propozycja odpowiedzi w pewnym stopniu 135 wskazań i 38 %, następnie raczej nie 13 wskazania i 4 % i nie miałoby to w ogóle wpływu na poprawę systemu zaledwie 11 wskazań, co daje 3 %.

Podobnie ukształtował się rozkład wyników II grupy respondentów. Ankietowani najczęściej dokonywali wyboru zdecydowanie tak, uzyskano odpowiedzi na poziomie 47 % (730 wskazań). Kolejną wybieraną w tej grupie była odpowiedź w pewnym stopniu na poziomie 43 % i 665 wskazań. Na trzecim miejscu respondenci tej grupy wskazali odpowiedź raczej nie z 114 wskazaniami i 7 %. Na ostatnim miejscu wskazywano odpowiedź nie miałoby to w ogóle wpływu na poprawę systemu z 36 wskazaniami, co daje 4 % odpowiedzi.

Szczegółowy rozkład odpowiedzi dotyczący występujących zagrożeń zaprezentowano w tabeli 4-31.

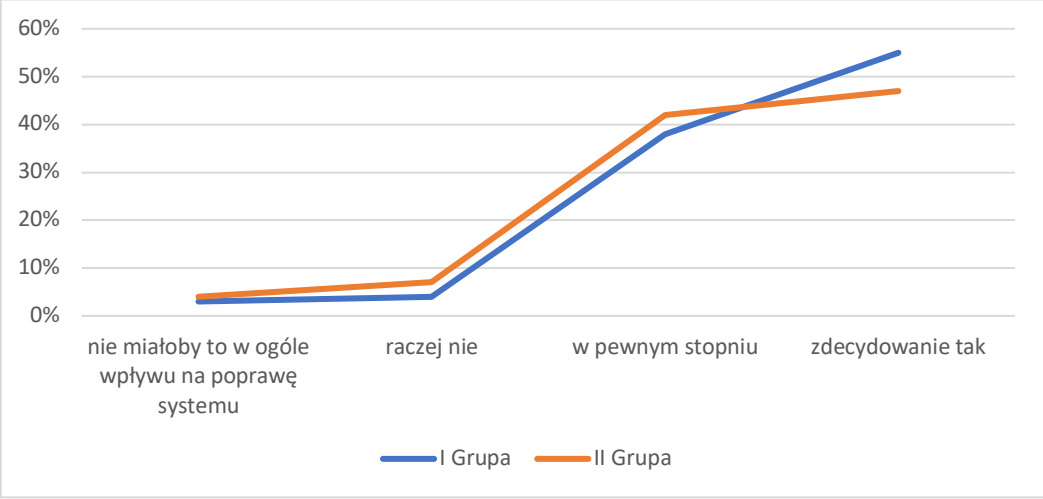
Tabela 4-31
Procentowy rozkład odpowiedzi dotyczący wpływu ujednolicenia systemów teleinformatycznych PSP na bezpieczeństwo systemu informacyjnego.

Odpowiedzi	I Grupa PRACOWNICY KW		II Grupa PRACOWNICY KM/KP		Ogółem	
	Struktura liczbowa	Struktura procentowa (%)	Struktura liczbowa	Struktura procentowa (%)	Struktura liczbowa	Struktura procentowa (%)
nie miałoby to w ogóle wpływu na poprawę systemu	11	3	36	3	47	3
raczej nie	13	4	114	7	127	6
w pewnym stopniu	135	38	665	43	800	42
zdecydowanie tak	193	55	730	47	923	49
Ogółem	352	100	1545	100	1897	100

Źródło: Opracowanie własne.

W celu dokładniejszego zobrazowania uzyskanych rozkładów udzielonych odpowiedzi z obu grup, wyniki zaprezentowano na wykresie 4-32

Wykres 4-32
Procentowy rozkład odpowiedzi obu grupach dotyczący wpływu ujednolicenia systemów teleinformatycznych PSP na bezpieczeństwo systemu informacyjnego.



Zaprezentowany, powyższy wykres wskazuje na niewielkie rozbieżności, które wynikają z udzielonych przez wszystkich ankietowanych odpowiedzi. W celu zbadania tejże istotności wykonano test współczynnika korelacji liniowej r- Pearsona.

Tabela 4-32
Rozkład odpowiedzi dotyczący wpływu ujednolicenia systemów teleinformatycznych PSP na bezpieczeństwo systemu informacyjnego.

Odpowiedzi	I Grupa KW	II Grupa KM/KP	Ogółem		
	x_i	y_i	x_i^2	y_i^2	$x_i * y_i$
Tak	11	36	121	1296	396
częściowo tak-wymaga udoskonalania	13	114	169	12996	1482
nie	135	665	18225	442225	89775
trudno powiedzieć	193	730	37249	532900	140890
Ogółem	$\sum_{i=3}^{n} x_i =$ 352	$\sum_{i=3}^{n} y_i =$ 1545	$\sum_{i=3}^{n} x_i^2 =$ 55764	$\sum_{i=3}^{n} y_i^2 =$ 989417	$\sum_{i=3}^{n} x_i * y_i =$ 232543
$\bar{x} = \frac{1}{n}\sum_{i=n}^{n} x_i = \frac{1}{4} * 352 \approx 88$ $x^2 \approx 7\,744$ | $\bar{y} = \frac{1}{n}\sum_{i=n}^{n} y_i = \frac{1}{4} * 1545 \approx 386$ $y^2 \approx 148\,996$					

Źródło: Opracowanie własne.

$$r = \frac{\frac{1}{n}\sum_{i=n}^{n} x_i y_i - xy}{\sqrt{(\frac{1}{n}\sum_{i=n}^{n} x_i^2 - x^2)(\frac{1}{n}\sum_{i=n}^{n} y_i^2 - y^2)}} = \frac{\frac{1}{4} * 232543 - 33\,968}{\sqrt{(\frac{1}{4} * 55764 - 7\,744)(\frac{1}{4} * 989417 - 148\,996)}} \approx 0{,}97$$

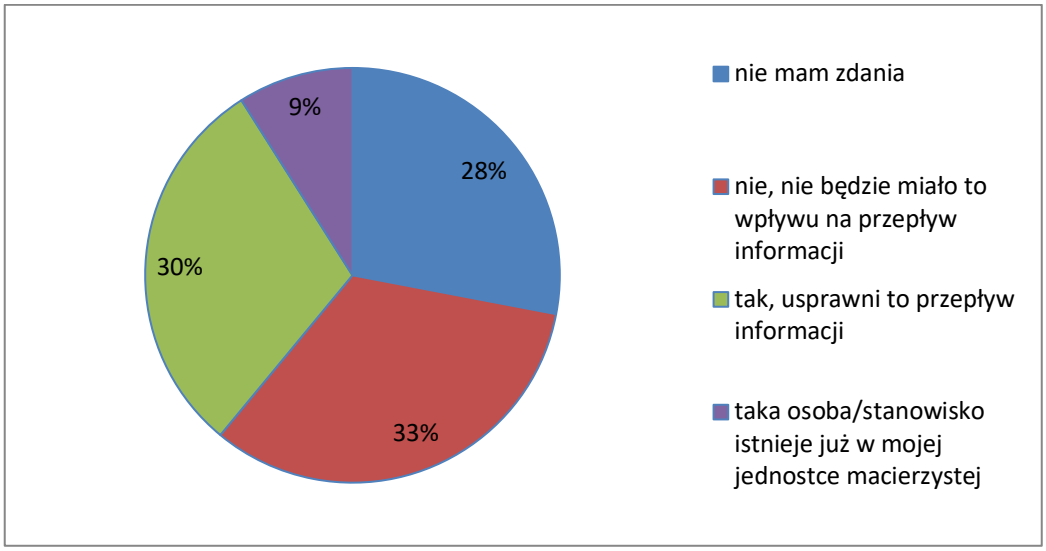
Przedstawiona powyższa analiza ukazuje, że współczynnik korelacji liniowej Pearsona wynosi r ≈ 0,97, co wskazuje na korelacje dodatnią o bardzo silnej zależności. Świadczy to o tym, iż wzrost wartości w udzielonych odpowiedziach jednej z grup powoduje wzrost wartości odpowiedzi drugiej z grup.

W ramach przeprowadzonych badań empirycznych poproszono respondentów o udzielenie odpowiedzi na pytanie siedemnaste (zał. 1): 17. *Czy Pani/Pana zdaniem zasadnym jest wyodrębnienie w macierzystej jednostce stanowiska/osoby odpowiedzialnej za przekazywanie informacji od kierownictwa do szczebla wykonawczego oraz zbieranie i przekazywanie informacji zwrotnych?*

W tym pytaniu badanym zaproponowano cztery warianty odpowiedzi, jednokrotnego wyboru. Ogólny rozkład odpowiedzi został zaprezentowany na wykresie 4-33, z którego wynika, iż najwięcej opiniodawców odpowiedziało się za wariantem, iż nie, nie będzie miało to wpływu na przepływ informacji, o czym świadczy 33 % uzyskanych odpowiedzi, na co złożyło się 609 wskazań. Następną z kolei wskazywaną odpowiedzią było, tak, usprawni to przepływ informacji 30 % (577 wskazań). 28 % ankietowanych

nie miało zdania w tym temacie (536 wskazania). Natomiast na odpowiedź taka osoba/stanowisko istnieje już w mojej jednostce macierzystej wskazało 9 % próby badawczej (175 wskazań).

Wykres 4-33
Procentowy rozkład odpowiedzi dotyczący wprowadzenia stanowiska odpowiedzialnego za przekazywanie informacji zwrotnych.



Źródło: Opracowanie własne.

Respondenci należący do I grupy najczęściej wskazywali na odpowiedź, iż nie, nie będzie miało to wpływu na przepływ informacji - 40 % (140 wskazań). Następną z kolei wskazywaną odpowiedzią było nie mam zdania – 27 % (96 wskazania). Odpowiedź, tak usprawni to przepływ informacji - 24 % (85 wskazań). Natomiast na odpowiedź taka osoba/stanowisko istnieje już w mojej jednostce macierzystej wskazało - 9 % próby badawczej (31 wskazań).

W II grupie ankietowanych odpowiedzi rozłożyły się nieco inaczej. Odpowiedź, tak usprawni to przepływ informacji - 32 % (492 wskazań). Następną w kolejności była iż nie, będzie miało to wpływu na przepływ informacji - 30 % (469 wskazań). Trzecią wybieraną odpowiedzią było nie mam zdania – 29 % (440 wskazania). Natomiast na odpowiedź taka osoba/stanowisko istnieje już w mojej jednostce macierzystej wskazało - 9 % próby badawczej (144 wskazań).

Szczegółowy rozkład danych odpowiedzi został ukazany w tabeli 4-33.

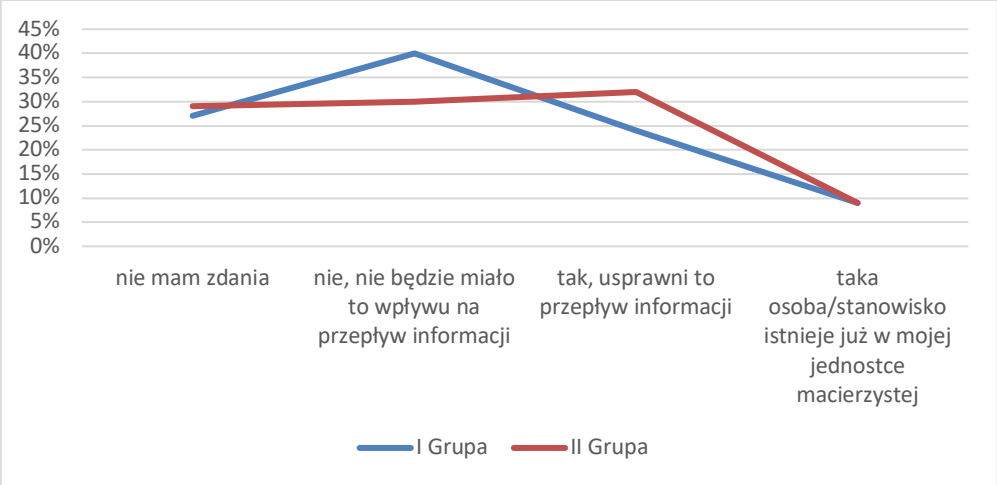
Tabela 4-33
Procentowy rozkład odpowiedzi dotyczący wprowadzenia stanowiska odpowiedzialnego za przekazywanie informacji zwrotnych.

Odpowiedzi	I Grupa PRACOWNICY KW		II Grupa PRACOWNICY KM/KP		Ogółem	
	Struktura liczbowa	Struktura procentowa (%)	Struktura liczbowa	Struktura procentowa (%)	Struktura liczbowa	Struktura procentowa (%)
nie mam zdania	96	27	440	29	536	28
nie, nie będzie miało to wpływu na przepływ informacji	140	40	469	30	609	33
tak, usprawni to przepływ informacji	85	24	492	32	577	30
taka osoba/stanowisko istnieje już w mojej jednostce macierzystej	31	9	144	9	175	9
Ogółem	352	100	1545	100	1897	100

Źródło: Opracowanie własne.

W celu dokładniejszego zobrazowania uzyskanych rozkładów udzielonych odpowiedzi z obu grup, wyniki zaprezentowano na wykresie 4-34.

Wykres 4-34
Procentowy rozkład odpowiedzi w obu grupach badawczych dotyczący wprowadzenia stanowiska odpowiedzialnego za przekazywanie informacji zwrotnych.



Zaprezentowany, powyższy wykres wskazuje na rozbieżności, które wynikają z udzielonych przez wszystkich ankietowanych odpowiedzi. W celu zbadania tejże istotności wykonano test współczynnika korelacji liniowej r- Pearsona.

Tabela 4-34
Rozkład odpowiedzi dotyczący wprowadzenia stanowiska odpowiedzialnego za przekazywanie informacji zwrotnych.

Odpowiedzi	I Grupa KW	II Grupa KM/KP	Ogółem		
	x_i	y_i	x_i^2	y_i^2	$x_i * y_i$
nie mam zdania	96	440	9216	193600	42240
nie, nie będzie miało to wpływu na przepływ informacji	140	469	19600	219961	65660
tak, usprawni to przepływ informacji	85	492	7225	242064	41820
taka osoba/stanowisko istnieje już w mojej jednostce macierzystej	31	144	961	20736	4464
Ogółem	$\sum_{i=3}^{n} x_i =$ 352	$\sum_{i=3}^{n} y_i =$ 1545	$\sum_{i=3}^{n} x_i^2 =$ 37002	$\sum_{i=3}^{n} y_i^2 =$ 676361	$\sum_{i=3}^{n} x_i * y_i =$ 154184
$\bar{x} = \frac{1}{n}\sum_{i=n}^{n} x_i = \frac{1}{4} * 352 \approx 88$ $x^2 \approx 7\,744$ | $\bar{y} = \frac{1}{n}\sum_{i=n}^{n} y_i = \frac{1}{4} * 1545 \approx 386$ $y^2 \approx 148\,996$					

Źródło: Opracowanie własne.

$$r = \frac{\frac{1}{n}\sum_{i=n}^{n} x_i y_i - xy}{\sqrt{(\frac{1}{n}\sum_{i=n}^{n} x_i^2 - x^2)(\frac{1}{n}\sum_{i=n}^{n} y_i^2 - y^2)}} = \frac{\frac{1}{4} * 154184 - 33\,968}{\sqrt{(\frac{1}{4} * 37002 - 7\,744)(\frac{1}{4} * 676361 - 148\,996)}} \approx 0{,}83$$

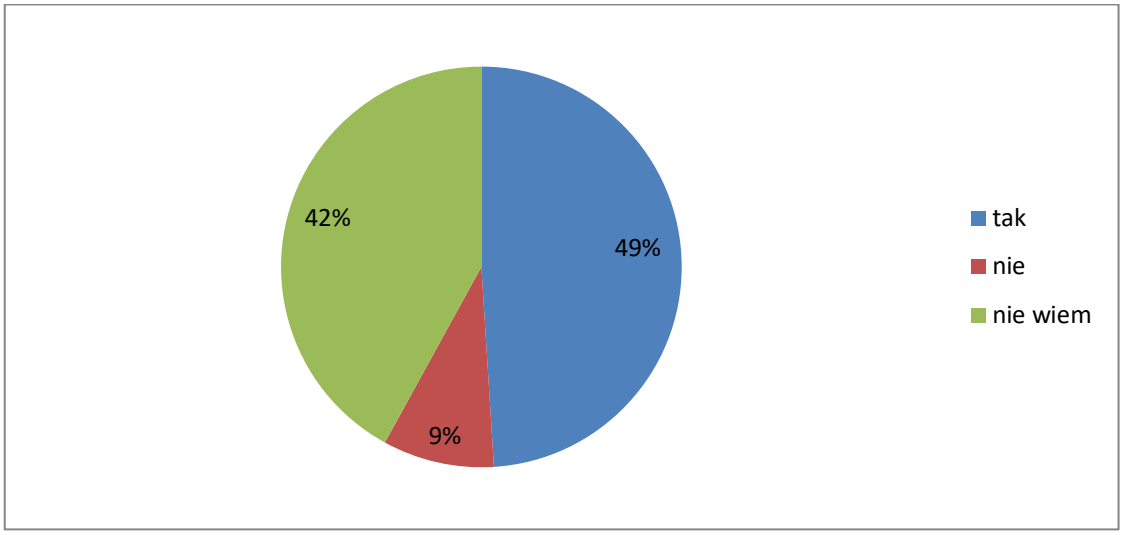
Obliczony współczynnik wynosi w przybliżeniu r = 0,83 i należy stwierdzić, iż jest to korelacja dodatnia o silnym wysokim charakterze. Świadczy to o występującej dość silnej zależnośc-tendencji pomiędzy przynależnością do grupy, a wskazywaniem danej odpowiedzi oraz oznacza to, iż wzrost wartości odpowiedzi jednej z grup wpływa na wzrost wartości odpowiedzi drugiej z grup (jednak występują minimalne rozbieżności pomiędzy poszczególnymi grupami).

W ramach przeprowadzonych badań empirycznych poproszono respondentów o udzielenie odpowiedzi na kolejne osiemnaste pytanie (zał. 1): 18. *Czy Pani/Pana zdaniem budowa chmury obliczeniowej dla PSP, tzn. dostarczanie przez Internet kluczowych usług obliczeniowych - w tym serwerów, pamięci masowej, baz danych i oprogramowania znacząco wpłynęłoby na poprawę funkcjonowania systemu informacyjnego?*

Badanym zaproponowano trzy warianty odpowiedzi, z których mogli dokonać jednokrotnego wyboru, tak, nie i nie wiem. Ogólny rozkład odpowiedzi został zaprezentowany na wykresie 4-35, z którego wynika, iż najwięcej opiniodawców odpowiedziało się za pierwszym wariantem odpowiedzi na tak, o czym świadczy 49 % uzyskanych odpowiedzi, na co złożyło się 924 wskazań. Stosunkowo mniej głosów respondentów uzyskał wariant odpowiedzi nie wiem 42 % i 800 wskazań,. Natomiast najmniej popularną była odpowiedź na nie, którą wskazało zaledwie 9 % próby badawczej, co stanowiło 173 wskazań.

Bardziej szczegółowy rozkład został ujęty w tabeli 4-35.

Wykres 4-35
Procentowy rozkład odpowiedzi dotyczący potrzeby budowy chmury obliczeniowej dla PSP.



Źródło: Opracowanie własne.

Respondenci należący do I grupy najczęściej wskazywali na odpowiedź nie wiem 50 % i 179 wskazań. Odpowiedź tak, potwierdzając potrzebę budowy chmury obliczeniowej PSP, uzyskała 40 %, co stanowiło 137 wskazania. Na odpowiedź negującą potrzebę wprowadzenia takiego rozwiązania zagłosowało jedynie 10 % ankietowanych z liczbą 36 wskazań.

Inaczej ukształtował się rozkład procentowy udzielonych odpowiedzi przez respondentów II grupy. Najwięcej odpowiedzi było na tak, która otrzymała 48 %, czyli 747 wskazań. Następnie na drugi miejscu z 661 wskazaniami i 43 % uplasował się wariant odpowiedzi nie wiem. Natomiast wariant trzeci nie z wynikiem 9 %, na co złożyły się 137 wskazania był najrzadziej wybieraną odpowiedzią wśród ankietowanych tej grupy.

Szczegółowy rozkład danych odpowiedzi został ukazany w tabeli 4-35.

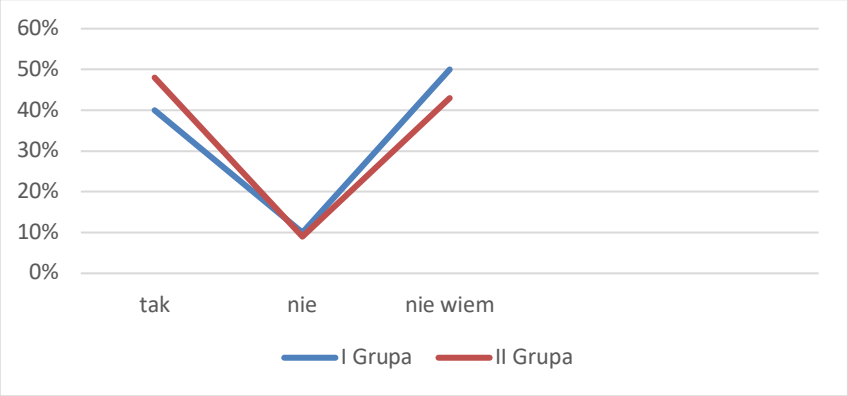
Tabela 4-35
Procentowy rozkład odpowiedzi dotyczący potrzeby budowy chmury obliczeniowej dla PSP.

Odpowiedzi	I Grupa PRACOWNICY KW		II Grupa PRACOWNICY KM/KP		Ogółem	
	Struktura liczbowa	Struktura procentowa (%)	Struktura liczbowa	Struktura procentowa (%)	Struktura liczbowa	Struktura procentowa (%)
Tak	137	40	747	48	884	56
Nie	36	10	137	9	173	11
nie wiem	179	50	661	43	840	33
Ogółem	352	100	1545	100	1897	100

Źródło: Opracowanie własne.

W celu dokładniejszego zobrazowania uzyskanych rozkładów udzielonych odpowiedzi z obu grup, wyniki zaprezentowano na wykresie 4-36.

Wykres 4-36
Procentowy rozkład odpowiedzi w obu grupach badawczych dotyczący potrzeby budowy chmury obliczeniowej dla PSP.



Zaprezentowany, powyższy wykres wskazuje na niewielkie rozbieżności, które wynikają z udzielonych przez wszystkich ankietowanych odpowiedzi. W celu zbadania tejże istotności wykonano test współczynnika korelacji liniowej r- Pearsona.

Tabela 4-36
Rozkład odpowiedzi dotyczący potrzeby budowy chmury obliczeniowej dla PSP.

Odpowiedzi	I Grupa KW	II Grupa KM/KP	Ogółem		
	x_i	y_i	x_i^2	y_i^2	$x_i * y_i$
Tak	137	747	18769	558009	102339
Nie	36	137	1296	18769	4932
nie wiem	179	661	32041	436921	118319
Ogółem	$\sum_{i=5}^{n} x_i =$ 352	$\sum_{i=5}^{n} y_i =$ 1545	$\sum_{i=5}^{n} x_i^2 =$ 52106	$\sum_{i=5}^{n} y_i^2 =$ 1013699	$\sum_{i=5}^{n} x_i * y_i =$ 225590
$\bar{x} = \frac{1}{n}\sum_{i=n}^{n} x_i = \frac{1}{3} * 352 \approx 117$ $x^2 \approx 13689$ | $\bar{y} = \frac{1}{n}\sum_{i=n}^{n} y_i = \frac{1}{3} * 1545 \approx 509$ $y^2 \approx 259\,081$					

Źródło: Opracowanie własne.

$$r = \frac{\frac{1}{n}\sum_{i=n}^{n} x_i y_i - xy}{\sqrt{(\frac{1}{n}\sum_{i=n}^{n} x_i^2 - x^2)(\frac{1}{n}\sum_{i=n}^{n} y_i^2 - y^2)}} = \frac{\frac{1}{3} * 225590 - 59044}{\sqrt{(\frac{1}{3} * 52106 - 13689)(\frac{1}{3} * 1013699 - 259\,081)}} \approx 0{,}91$$

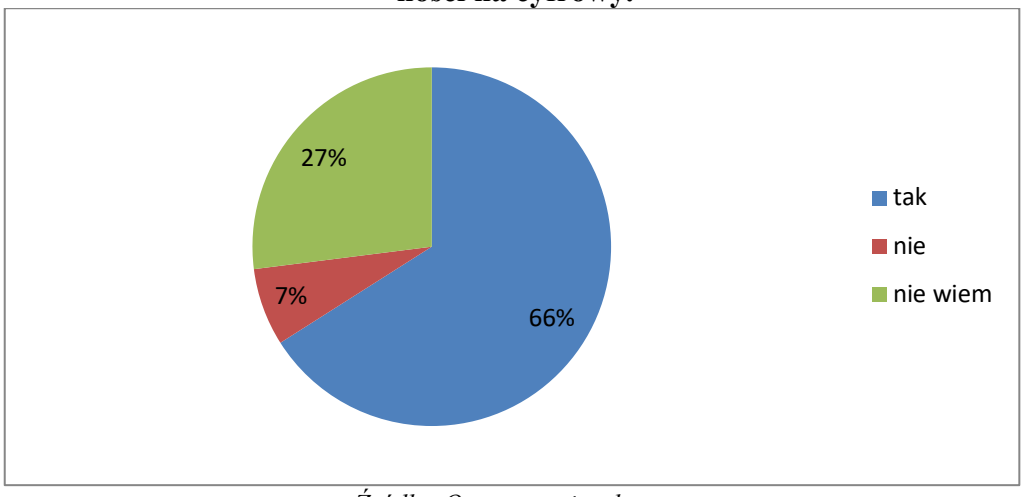
Obliczony współczynnik wynosi w przybliżeniu r ≈ 0,91. Można stwierdzić, iż jest to korelacja dodatnia o bardzo wysokim charakterze. Świadczy to o występującej dość silnej zależności pomiędzy przynależnością do grupy a wskazywaniem odpowiedzi. Oznacza to, iż wzrost wartości odpowiedzi jednej z grup wpływa na wzrost wartości odpowiedzi drugiej z grup.

W ramach przeprowadzonych badań empirycznych poproszono respondentów o udzielenie odpowiedzi na przedostatnie dziewiętnaste pytanie (zał. nr 1) 19. *Czy Pani/Pana zdaniem migracja usług systemów łączności radiowej z analogowych do cyfrowych jest dobrym kierunkiem?*

Respondenci mieli do wyboru następujące warianty odpowiedzi: tak, nie i nie wiem. Ogólny rozkład odpowiedzi został zilustrowany na wykresie 4-37. Wynika z niego, iż najwięcej wskazań otrzymała pierwsza zaproponowana możliwość tak, potwierdzająca potrzebę migracji usług łączności na system radiowy. Dowodem tego jest procentowy udział kształtujący się na poziomie aż 66 % odpowiedzi, co stanowi 1245 wskazań respondentów obu grup. Na odpowiedź przeczącą zdecydowała się tylko grupa 7 % ankietowanych, co stanowiło 135 ze wszystkich wskazań. Natomiast osoby, które nie miały wiedzy w tym zakresie stanowiły 27 %, na co złożyło się 517 wskazań wariantu odpowiedzi – nie wiem.

Szczegółowy rozkład odpowiedzi został ukazany w tabeli 4-37.

Wykres 4-37
Procentowy rozkład odpowiedzi dotyczący potrzeby kierunku migracji systemu łączności na cyfrowy.



Źródło: Opracowanie własne.

Respondenci należący do I grupy najczęściej wskazywali na odpowiedź potwierdzającą potrzebę zmiany na system cyfrowy, gdyż odpowiedź ta uzyskała aż 67 %, co stanowiło 236 wskazania. Następnie wariant odpowiedzi nie wiem, wskazało 100 osób, co dało wynik 28 % respondentów. Natomiast na wariant odpowiedzi nie, odpowiedziało zaledwie 5 % ankietowanych z liczbą 16 wskazań.

Bardzo podobnie kształtował się układ odpowiedzi udzielonych przez respondentów II grupy. Najwięcej odpowiedzi otrzymała odpowiedź tak, o czym świadczy 65 %, czyli 1009 wskazań. Następnie 27 % uzyskał wariant odpowiedzi nie wiem z liczbą 417 wskazań. Wariant z odpowiedzią nie uplasował się na ostatnim miejscu z wynikiem 8 %, na co złożyły się 119 wskazań.

Szczegółowy rozkład danych odpowiedzi został ukazany w tabeli 4-37

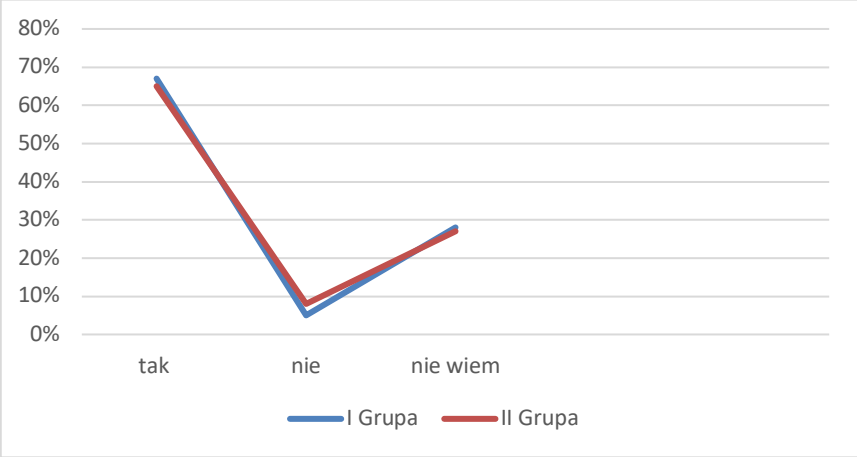
Tabela 4-37
Procentowy rozkład odpowiedzi dotyczący potrzeby kierunku migracji systemu łączności na cyfrowy.

Odpowiedzi	I Grupa PRACOWNICY KW		II Grupa PRACOWNICY KM/KP		Ogółem	
	Struktura liczbowa	Struktura procentowa (%)	Struktura liczbowa	Struktura procentowa (%)	Struktura liczbowa	Struktura procentowa (%)
Tak	236	67	1009	65	1245	66
Nie	16	5	119	8	135	7
nie wiem	100	28	417	27	517	27
Ogółem	352	100	1545	100	1897	100

Źródło: Opracowanie własne.

W celu dokładniejszego zobrazowania uzyskanych rozkładów udzielonych odpowiedzi z obu grup, wyniki zaprezentowano na wykresie 4-38.

Wykres 4-38
Procentowy rozkład odpowiedzi w obu grupach badawczych dotyczący potrzeby kierunku migracji systemu łączności na cyfrowy.



Zaprezentowany, powyższy wykres wskazuje na bardzo niewielkie rozbieżności, które wynikają z udzielonych przez wszystkich ankietowanych odpowiedzi. W celu zbadania tejże istotności wykonano test współczynnika korelacji liniowej r- Pearsona.

Tabela 4-38
Rozkład odpowiedzi dotyczący potrzeby kierunku migracji systemu łączności na cyfrowy.

Odpowiedzi	I Grupa KW	II Grupa KM/KP	Ogółem		
	x_i	y_i	x_i^2	y_i^2	$x_i * y_i$
Tak	236	1009	55696	1018081	238124
Nie	16	119	256	14161	1904
nie wiem	100	417	10000	173889	41700
Ogółem	$\sum_{i=3}^{n} x_i =$ 352	$\sum_{i=3}^{n} y_i =$ 1545	$\sum_{i=3}^{n} x_i^2 =$ 65952	$\sum_{i=3}^{n} y_i^2 =$ 1206131	$\sum_{i=3}^{n} x_i * y_i =$ 281728
$\bar{x} = \frac{1}{n}\sum_{i=n}^{n} x_i = \frac{1}{3} * 352 \approx 117$ $x^2 \approx 13689$ | $\bar{y} = \frac{1}{n}\sum_{i=n}^{n} y_i = \frac{1}{3} * 1545 \approx 509$ $y^2 \approx 259\,081$					

Źródło: Opracowanie własne.

$$r = \frac{\frac{1}{n}\sum_{i=n}^{n} x_i y_i - xy}{\sqrt{(\frac{1}{n}\sum_{i=n}^{n} x_i^2 - x^2)(\frac{1}{n}\sum_{i=n}^{n} y_i^2 - y^2)}} = \frac{\frac{1}{3} * 281728 - 59044}{\sqrt{(\frac{1}{3} * 65952 - 13689)(\frac{1}{3} * 1206131 - 259081)}} \approx 0{,}99$$

Podobnie jak w przypadku wcześniejszych pytań po przeprowadzeniu testu współczynnika korelacji liniowej r- Pearsona, otrzymano wynik r ≈ 0,99, co świadczy, że pomiędzy poszczególnymi grupami występuje bardzo silna zależność i mówimy o korelacji dodatniej. Wyniki świadczą o tym, iż wzrost wartości w odpowiedziach u jednej z grup powoduje wzrost wartości odpowiedzi w grupie drugiej.

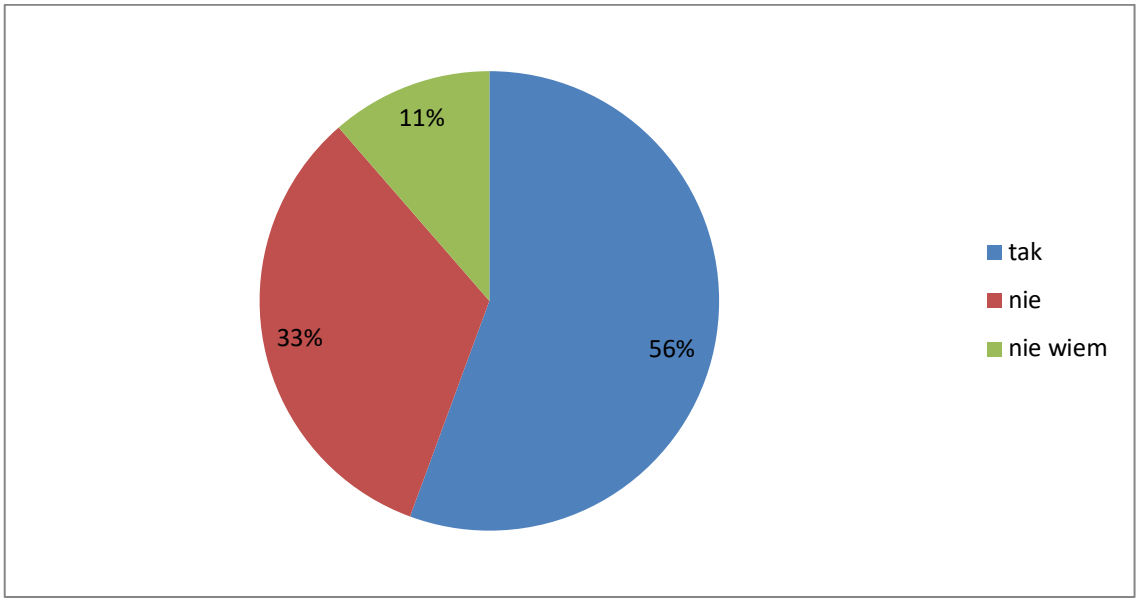
W ramach przeprowadzonych badań empirycznych poproszono respondentów o udzielenie odpowiedzi na ostatnie dwudzieste pytanie (zał. 1): 20. *Czy Pani/Pana zdaniem zmiana architektury Systemu Wspomagania Decyzji PSP z rozproszonej na scentralizowaną oraz dodanie nowych modułów (m.in. współpracy z jednostkami Ochotniczych Straży Pożarnych, współpracy z innymi instytucjami współdziałającymi) usprawni procesy obsługi zdarzeń?*

Badanym zaproponowano trzy warianty odpowiedzi, jednokrotnego wyboru, tak, nie, i nie wiem w wyniku czego uzyskano łącznie 1897 wskazań. Ogólny rozkład odpowiedzi został zaprezentowany na wykresie 4-39, z którego wynika, iż najwięcej opiniodawców odpowiedziało się za pierwszym wariantem odpowiedzi na tak, o czym świadczy

56 % uzyskanych odpowiedzi, na co złożyło się 1055 wskazań. Mniej głosów respondentów uzyskały wariant odpowiedzi nie wiem 33 % i 626 wskazań,. Natomiast najmniej popularną była odpowiedź na nie, którą wskazało 11 % próby badawczej, co stanowiło 216 wskazań.

Bardziej szczegółowy rozkład został ujęty w tabeli 4-39.

Wykres 4-39
Procentowy rozkład odpowiedzi dotyczący zmiany architektury SWD PSP z rozproszonej na scentralizowaną.



Źródło: Opracowanie własne.

Respondenci należący do I grupy najczęściej wskazywali na odpowiedź tak, potwierdzając potrzebę scentralizowania architektury systemu SWD PSP – odpowiedź ta uzyskała 47 %, co stanowiło 167 wskazania. Na drugim miejscu uplasował się wariant odpowiedzi nie wiem, gdzie wskazania takiego dokonało 40% respondentów, na co złożyło się 141 wskazań. Na trzeci wariant z możliwych odpowiedzi nie, który był za utrzymaniem architektury rozproszonej zdecydowało się 13 % ankietowanych, 44 wskazania.

Inaczej ukształtował się rozkład procentowy udzielonych odpowiedzi przez respondentów II grupy. Najwięcej odpowiedzi, tak jak w I grupie, otrzymała odpowiedź na tak, o czym świadczy 58 %, czyli 888 wskazań. Następnie na drugi miejscu z 485 wskazaniami i 31 % uplasował się wariant odpowiedzi nie wiem. Natomiast wariant trzeci nie z wynikiem 11 %, na co złożyły się 172 wskazania był najrzadziej wybieraną odpowiedzią wśród ankietowanych tej grupy.

Szczegółowy rozkład danych odpowiedzi został ukazany w tabeli 4-39.

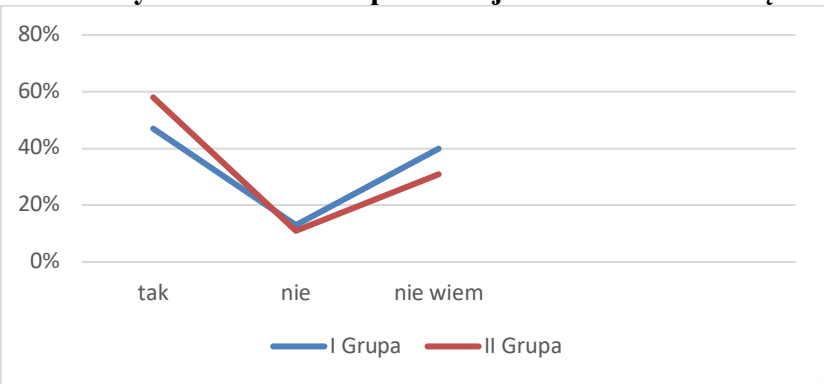
Tabela 4-39
Procentowy rozkład odpowiedzi dotyczący zmiany architektury SWD PSP z rozproszonej na scentralizowaną.

Odpowiedzi	I Grupa PRACOWNICY KW		II Grupa PRACOWNICY KM/KP		Ogółem	
	Struktura liczbowa	Struktura procentowa (%)	Struktura liczbowa	Struktura procentowa (%)	Struktura liczbowa	Struktura procentowa (%)
Tak	167	47	888	58	1055	56
Nie	141	13	485	11	216	11
nie wiem	44	40	172	31	626	33
Ogółem	352	100	1545	100	1897	100

Źródło: Opracowanie własne.

W celu dokładniejszego zobrazowania uzyskanych rozkładów udzielonych odpowiedzi z obu grup, wyniki zaprezentowano na wykresie 4-40.

Wykres 4-40
Procentowy rozkład odpowiedzi w obu grupach badawczych dotyczący zmiany architektury SWD PSP z rozproszonej na scentralizowaną.



Zaprezentowany, powyższy wykres wskazuje na niewielkie rozbieżności, które wynikają z udzielonych przez wszystkich ankietowanych odpowiedzi. W celu zbadania tejże istotności wykonano test współczynnika korelacji liniowej r- Pearsona.

Tabela 4-40
Rozkład odpowiedzi dotyczący zmiany architektury SWD PSP z rozproszonej na scentralizowaną.

Odpowiedzi	I Grupa KW	II Grupa KM/KP	Ogółem		
	x_i	y_i	x_i^2	y_i^2	$x_i * y_i$
Tak	167	888	27889	788544	148296
Nie	141	485	19881	235225	68385
nie wiem	44	172	1936	29584	7568
Ogółem	$\sum_{i=5}^{n} x_i =$ 352	$\sum_{i=5}^{n} y_i =$ 1545	$\sum_{i=5}^{n} x_i^2 =$ 49706	$\sum_{i=5}^{n} y_i^2 =$ 1053353	$\sum_{i=5}^{n} x_i * y_i =$ 224249
$\bar{x} = \frac{1}{n}\sum_{i=n}^{n} x_i = \frac{1}{3} * 352 \approx 117$ $x^2 \approx 13689$ | $\bar{y} = \frac{1}{n}\sum_{i=n}^{n} y_i = \frac{1}{3} * 1545 \approx 509$ $y^2 \approx 259\,081$					

Źródło: Opracowanie własne.

$$r = \frac{\frac{1}{n}\sum_{i=n}^{n} x_i y_i - xy}{\sqrt{(\frac{1}{n}\sum_{i=n}^{n} x_i^2 - x^2)(\frac{1}{n}\sum_{i=n}^{n} y_i^2 - y^2)}} = \frac{\frac{1}{3} * 224249 - 59044}{\sqrt{(\frac{1}{3} * 49706 - 13689)(\frac{1}{3} * 1053353 - 259\,081)}} \approx 0{,}92$$

Obliczony współczynnik wynosi w przybliżeniu 0,92. Można stwierdzić, iż jest to korelacja dodatnia o bardzo wysokim charakterze. Świadczy to o występującej dość silnej zależności pomiędzy przynależnością do grupy a wskazywaniem odpowiedzi. Oznacza to, iż wzrost wartości odpowiedzi jednej z grup wpływa na wzrost wartości odpowiedzi drugiej z grup.

4.2 KONCEPCJA ROZWOJU SYSTEMU INFORMACYJNEGO W PAŃSTWOWEJ STRAŻY POŻARNEJ W ASPEKCIE BEZPIECZNEJ, PEWNEJ I SPRAWNEJ KOMUNIKACJI NA WIELU PŁASZCZYZNACH.

4.2.1 STRATEGIA CYFRYZACJI PSP – CELE KONCEPCJI ROZWOJU SYSTEMU WYMIANY INFORMACJI

Koncepcja cyfryzacji Państwowej Straży Pożarnej, ze szczególnym uwzględnieniem bezpiecznej, pewnej i sprawnej komunikacji na wielu płaszczyznach, ma w pierwszej kolejności za zadanie zoptymalizowanie procesów zachodzących podczas działań ratowniczych, traktując priorytetowo funkcjonowanie stanowisk kierowania PSP oraz sztabów PSP - kierujących działaniami ratowniczymi na każdym z poziomów, ze szczególnym uwzględnieniem Systemu Wspomagania Decyzji Państwowej Straży Pożarnej. Zakłada ona osiągnięcie trzech poniższych celów:

- przeniesienie kluczowych usług do chmury obliczeniowej,
- migrację systemów łączności radiowej z usług analogowych do cyfrowych,
- budowę nowego scentralizowanego SWD PSP.

Dzięki powyższym krokom możliwym stanie się również zunifikowanie sposobów postępowania w zakresie uruchamiania awaryjnych planów ewakuacji dyżurnych operacyjnych i dyspozytorów oraz sprzętu technicznego w miejsca zastępcze.

Wdrożenie koncepcji w ramach wskazanych powyżej celów, wymusza również przeprowadzanie:

- zmian prawno-formalnych w zakresie odpowiednich procedur, zasad, wytycznych, instrukcji, metodyk, szkoleń, itp.,
- szkoleń dla użytkowników, pozwalających na pełne wykorzystanie nowych technologii i systemów.

Cel I – budowa chmury obliczeniowej państwowej straży pożarnej, w tym zorganizowanie w jej przestrzeni kluczowych usług.

Podstawowym celem budowy chmury obliczeniowej Państwowej Straży Pożarnej jest stworzenie środowiska hybrydowego wraz z przeniesieniem do niej kluczowych usług, które są jednymi z najważniejszych celów strategii cyfryzacji stanowisk kierowania Państwowej Straży Pożarnej, w szczególności pod kątem:

- Skalowalności: chmura obliczeniowa pozwala na elastyczne dostosowywanie zasobów obliczeniowych w zależności od potrzeb. Dzięki temu Państwowa Straż Pożarna może zwiększać lub zmniejszać zasoby w zależności od natężenia działań ratunkowych.
- Dostępności: chmura obliczeniowa umożliwia dostęp do aplikacji i danych z dowolnego miejsca i o dowolnej porze. Dzięki temu strażacy mogą uzyskać dostęp do potrzebnych informacji i aplikacji niezależnie od tego, gdzie się znajdują.
- Bezpieczeństwa: chmura obliczeniowa zapewnia zaawansowane zabezpieczenia, takie jak szyfrowanie danych, uwierzytelnianie i kontrola dostępu, co pozwala na ochronę ważnych danych i informacji.
- Niższych kosztów: przeniesienie usług do chmury obliczeniowej pozwala na zmniejszenie kosztów związanych z zakupem, utrzymaniem i aktualizacją sprzętu i oprogramowania.
- Współdzielenia danych: chmura obliczeniowa umożliwia łatwe współdzielenie danych i aplikacji między różnymi jednostkami Państwowej Straży Pożarnej, co pozwala na lepszą koordynację działań ratunkowych.
- Innowacyjności: Przeniesienie usług do chmury pozwala na wykorzystanie nowych technologii i usług, które pozwalają na automatyzację i usprawnienie procesów, co zwiększa efektywność działań ratunkowych i pozwala na lepsze zarządzanie sytuacjami awaryjnymi.

Przeniesienie kluczowych usług do chmury obliczeniowej pozwoli na lepsze wykorzystanie zasobów, usprawnienie procesów, zwiększenie bezpieczeństwa i redukcję kosztów. Dzięki temu Państwowa Straż Pożarna będzie mogła jeszcze bardziej skupić się na swoich podstawowych zadaniach, takich jak ratowanie życia i zdrowia ludzi, mienia

i środowiska, wykorzystując do tego celu nowoczesne technologie usprawniające te działania.

Chmura obliczeniowa PSP mogłaby stać się swoistą platformą, do wykorzystania nowoczesnych funkcjonalności i rozwiązań takich jak:

1. Usługi katalogowe Microsoft Active Directory:

Wdrożenie usług katalogowych Microsoft AD jako podwalin pod uruchomienie systemów wspomagających działania stanowisk kierowania PSP, sztabów PSP, kierujących działaniami ratowniczymi na każdym z poziomów, ze szczególnym uwzględnieniem Systemu Wspomagania Decyzji Państwowej Straży Pożarnej. Państwowa Straż Pożarna jest jednym z najważniejszych podmiotów odpowiedzialnych za bezpieczeństwo publiczne w Polsce. W celu zapewnienia jak najlepszej jakości usług i skutecznego zarządzania swoimi zasobami niezbędnym staje się wdrożenie system Microsoft Active Directory. Active Directory to rozwiązanie do zarządzania użytkownikami, komputerami i innymi zasobami w sieciach komputerowych. Dzięki wdrożeniu Active Directory, Państwowa Straż Pożarna może z centralnego miejsca zarządzać dostępem do plików, drukarek, aplikacji i innych zasobów sieciowych. System taki pozwala również na łatwiejsze zarządzanie kontami użytkowników, co oznacza szybsze i łatwiejsze tworzenie, usuwanie i zmienianie haseł dla swoich pracowników. Dodatkowo pozwala również na lepsze zabezpieczenie danych i aplikacji poprzez uwierzytelnianie i autoryzację użytkowników. Celem tego przedsięwzięcia jest poprawa efektywności działania strażaków oraz zwiększenie bezpieczeństwa danych gromadzonych w systemach teleinformatycznych.

Ponadto zastosowanie narzędzi Microsoft 365 umożliwi pracownikom dostęp do aplikacji i rozwiązań takich jak poczta elektroniczna, kalendarz oraz programy do tworzenia dokumentów z dowolnego miejsca i o każdej porze. To znacznie ułatwiło koordynację działań oraz udostępnianie informacji między jednostkami straży pożarnej.

Azure AD natomiast pozwoli na centralizację i usprawnienie zarządzania dostępem do danych i aplikacji. Dzięki temu strażacy będą mogli logować się do swoich kont jednym loginem i hasłem, a także korzystać z danych zabezpieczonych przez system uwierzytelniania dwuskładnikowego. Wdrożenie tych rozwiązań pozwoli na skuteczniejsze i bardziej efektywne działanie, co przełoży się na poprawę jakości i efektywności realizowania ustawowych zadań. Jest to również ważny krok w kierunku cyfryzacji PSP, co w konsekwencji pozwoli na lepsze wykorzystanie nowoczesnych technologii w działaniach ratowniczych.

2. Web OpenDroneMap (WEBODM) zwane 3D MAP:

Państwowa Straż Pożarna w Polsce coraz częściej wykorzystuje bezzałogowe statki powietrzne (BSP) do prowadzenia swoich działań. Loty realizowane przez BSP pozwalają na uzyskanie dokładnych i aktualnych informacji o miejscu zdarzenia, co przyczynia się do lepszej koordynacji działań i skuteczniejszej ochrony ludzi i mienia. Aby ułatwić przetwarzanie i analizę danych z lotów bezzałogowych, należy uruchomić środowisko Web OpenDroneMap (WEBODM) zwane 3D MAP. WEBODM to otwarty i darmowy system do przetwarzania danych z lotów BSP dla wszystkich strażaków PSP. Jest to aplikacja internetowa, która pozwala na przetwarzanie zdjęć lotniczych w celu wygenerowania modeli 3D, ortofotomap, punktów chmury i innych produktów. Dzięki temu, funkcjonariusze PSP mogą szybko i łatwo przetwarzać dane z lotów BSP, co pozwala na lepszą koordynację działań i szybszą reakcję na zagrożenia. Uruchomienie środowiska 3DMAP jest ważnym krokiem w kierunku wykorzystania nowoczesnych technologii w działaniach Państwowej Straży Pożarnej. Dzięki temu, Straż Pożarna będzie mogła realizować fotogrametrię w swoich działaniach, co pozwoli na uzyskanie dokładnych i aktualnych informacji o terenie, co przyczyni się do lepszej koordynacji działań i skuteczniejszej ochrony ludzi i mienia.

3. System typu „WIKI”:

Aby zwiększyć efektywność i skuteczność prowadzonych działań należy rozpocząć wdrażanie systemu typu „WIKI”, jako miejsce składowania danych operacyjnych. System WIKI to narzędzie do tworzenia i zarządzania treścią w formie stron internetowych. Jest to system łatwy w obsłudze, który pozwala na tworzenie i edycję stron przez wielu użytkowników jednocześnie. Dzięki temu, formacja jaką jest Straż Pożarna będzie mogła szybko i łatwo przechowywać i udostępniać dane operacyjne, takie jak plany działań, instrukcje, raporty i inne ważne informacje. Wdrożenie systemu WIKI pozwoli komendom i jednostką ratowniczo-gaśniczym PSP na lepszą koordynację działań i szybszą reakcję na zagrożenia. Będzie to również ułatwiać komunikację między różnymi jednostkami Straży Pożarnej, a także umożliwi lepsze zarządzanie zasobami i planowanie działań. Ogólnie rzecz biorąc, uruchomienie i wdrożenie systemu WIKI jako miejsca składowania danych operacyjnych dla Państwowej Straży Pożarnej jest dobrym krokiem w kierunku usprawnienia działań i poprawy efektywności działań tej instytucji.

4. Geograficzny System Informacji - GeoPortal PSP na bazie narzędzia ArcGis:

GeoPortal PSP na bazie ArcGis jest to narzędzie, które pozwala na tworzenie, udostępnianie i zarządzanie mapami i aplikacjami geograficznymi. Jest to rozwiązanie przeznaczone dla organizacji, które chcą wykorzystać potencjał danych geograficznych do podejmowania lepszych decyzji. Wdrożenie takiego systemu w Państwowej Straży Pożarnej pozwoli tworzyć i udostępniać mapy i aplikacje geograficzne związane z działaniami ratowniczymi. System ArcGIS Server pozwoli Straży Pożarnej na lepsze koordynowanie działań ratowniczych, a także na szybszą reakcję na zagrożenia. Oferuje on wiele różnych możliwości w zakresie zarządzania danymi geograficznymi, takich jak: tworzenie i udostępnianie map online, możliwość przesyłania danych w czasie rzeczywistym, zarządzanie dostępem do danych z poziomu aplikacji, tworzenie aplikacji mobilnych i internetowych, analizowanie danych przestrzennych. Wdrożenie systemu ArcGIS Server pozwoli Straży Pożarnej na lepsze wykorzystanie danych geograficznych w swoich działaniach ratowniczych, co przełoży się na skuteczniejszą ochronę ludzi i mienia. System planowany jest jako wiodące rozwiązanie na potrzeby wizualizacji danych w ramach systemu SWD-PSP.

GeoPortal funkcjonował będzie w ramach Geograficznego Systemu Informacji (GIS) wspomagającego i uzupełniającego dotychczas wykorzystywane w Państwowej Straży Pożarnej oprogramowanie w celach realizacji zadań związanych z analizą operacyjną dot. funkcjonowania oraz organizacji krajowego systemu ratowniczo-gaśniczego m.in. w zakresie:

- zobrazowania na mapach oraz prowadzenia analiz funkcjonowania ksrg na obszarze powiatu, województwa i kraju,
- zobrazowania na mapach oraz prowadzenia analiz w zakresie rozwoju ratownictwa specjalistycznego, w tym technicznego, wodno-nurkowego, wysokościowego, chemicznego, ekologicznego, medycznego, poszukiwawczo-ratowniczego oraz grup sonarowych i zespołów dronowych,
- prowadzenia analiz w zakresie dostępności zasobów PSP tworzących moduły ochrony ludności, przewidzianych do działań międzynarodowych
- zobrazowania na mapach prowadzenia akcji i/lub ćwiczeń kierowanych przez PSP na terenie kraju
- zobrazowania na mapach prowadzenia międzynarodowych działań realizowanych przez PSP wynikających z wiążących Rzeczpospolitą Polską umów międzynarodowych oraz odrębnych przepisów,
- opracowywania analiz zagrożeń oraz analiz zabezpieczenia operacyjnego,

- ustalanie obszarów chronionych dla specjalistycznych grup ratowniczych oraz dla podmiotów ksrg przewidzianych do realizacji zadań poza terenem własnego działania.
- wyznaczania obszarów, dla których prawdopodobny czas przybycia do zdarzenia pierwszych i kolejnych sił i środków podmiotów ksrg wynosi odpowiednio do 8 minut i do 15 minut, w celu wyznaczenia dla nich obszarów chronionych lub ich zmiany,
- określenia dla każdej dziedziny ratownictwa najbardziej prawdopodobnego czasu przybycia pierwszych i kolejnych specjalistycznych grup ratowniczych w celu wyznaczenia dla nich obszarów chronionych lub ich zmiany,
- wyznaczenia miejsc, obiektów i terenów o utrudnionych warunkach prowadzenia działań ratowniczych i niskim poziomie zabezpieczenia operacyjnego,
- tworzenia map zagrożeń w obszarach powiatu, województwa i kraju.

Koncepcja systemu zakłada upowszechnianie funkcjonalności systemu GIS poprzez wewnętrzny serwis Internetowy (intranetowy), współdzielenie zasobów i wyników geoanaliz przez użytkowników różnych poziomów zaawansowania, w trybie dostarczonej określonej liczby licencji. Oprogramowanie GIS ma zapewnić dostęp do narzędzi przetwarzania danych (tabelarycznych, wektorowych i rastrowych) oraz pracy z referencyjnymi podkładami mapowymi. Dodatkowo system będzie zapewniał integrację i konwersję danych pochodzących z różnych źródeł i rejestrów, w różnych formatach, wykonywanie analiz geostatystycznych oraz interpolację danych, a także ich wewnętrzną publikacje. Dane przestrzenne będą pochodzić z następujących obszarów tematycznych: jednostki administracyjne, strefy ekonomiczne, działki ewidencyjne, budynki, adresy i dane demograficzne, sieci transportowe, stacje BTS, ukształtowanie terenu, ortofotomapy, mapy topograficzne i niestandardowe opracowania tematyczne, a także dane OSM.

5. System zarządzania procesami biznesowymi (Business Process Manager System) – BPMS:

System tego rodzaju pozwoli na cyfryzację procesów wewnętrznych organizacji, co oznacza automatyzację i usprawnienie wielu czynności, takich jak cyfrowy obieg dokumentów i spraw, rejestracja zgłoszeń, przydzielanie zadań i raportowanie. System ten powinien być oparty na architekturze typu low-code/no-code, co oznacza, że jest on łatwy w obsłudze i nie wymaga specjalistycznej wiedzy informatycznej od użytkowników. Wdrożenie systemu zarządzania procesami biznesowymi pozwoli Straży Pożarnej na lepszą koordynację działań i szybszą reakcję na zagrożenia. Będzie to również ułatwiać komunikację między

różnymi jednostkami Straży Pożarnej, a także umożliwi lepsze zarządzanie zasobami i planowanie działań.

6. Narzędzia i usługi teleinformatyczne dla usprawnienia procesów PSP:

Wdrożenie powyższych rozwiązań umożliwi nadanie formy wielu usługom i narzędziom, dzięki który efektywniejszym stanie się dysponowanie zasobów ratowniczych do działań na terenie kraju, jak i poza jego granicami, poprzez zbudowanie:

- narzędzi informatycznych umożliwiających przeprowadzanie analiz zasobów danych z przypisaniem zarówno danym jak i wynikom analiz przestrzennej formy, w postaci wizualizacji tzw. mapy, a także animacji zapisanej w postaci filmu, w tym wytworzenie dedykowanego oprogramowania określanego powszechnie jako GIS (Geograficzny System Informacji),
- aplikacji do monitoringu poziomu gotowości operacyjnej grup specjalistycznych funkcjonujących na terenie kraju w ramach centralnego odwodu operacyjnego krajowego systemu ratowniczo-gaśniczego:
  - Specjalistycznych grup ratownictwa wodno-nurkowego,
  - Specjalistycznych grup ratownictwa wysokościowego,
  - Specjalistycznych grup ratownictwa chemiczno-ekologicznego,
  - Specjalistycznych grup ratownictwa technicznego,
  - Specjalistycznych grup poszukiwawczo-ratowniczych,
  - Specjalistycznych grup sonarowych,
  - Specjalistycznych grup dronowych.
- aplikacji do monitoringu poziomu gotowości operacyjnej kompani szkolnych funkcjonujących na terenie kraju w ramach centralnego odwodu operacyjnego krajowego systemu ratowniczo-gaśniczego:
  - Szkoły Głównej Służby Pożarniczej w Warszawie,
  - Centralnej Szkoły Państwowej Straży Pożarnej w Częstochowie,
  - Szkoły Aspirantów Państwowej Straży Pożarnej w Poznaniu,
  - Szkoły Aspirantów Państwowej Straży Pożarnej w Krakowie,
  - Szkoły Podoficerskiej Państwowej Straży Pożarnej w Bydgoszczy.
- aplikacji do monitoringu gotowości operacyjnej modułów ochrony ludności przeznaczonych do działań poza granicami kraju:
  - Modułów gaszenia pożarów lasów z ziemi z użyciem pojazdów,
  - Modułów pomp wysokiej wydajności,

- Modułów wykrywania skażeń chemicznych, biologicznych, radiologicznych i jądrowych oraz pobierania próbek,
- Modułów grupy poszukiwawczo-ratowniczej przeznaczonej do działań na terenach miejskich.

- aplikacji do monitoringu poziomu gotowości operacyjnej statków powietrznych służb, instytucji i podmiotów, które na bazie stosownych porozumień wykorzystywane są przez Państwową Straż Pożarną do działań ratowniczych i ratowniczo-gaśniczych:
  - Policji,
  - Straży Granicznej,
  - Sił Zbrojnych RP,
  - Lotniczego Pogotowia Ratunkowego,
  - Polskich Sieci Elektroenergetycznych.
- narzędzi teleinformatycznych pozwalających na dysponowanie i zarządzanie siłami i środkami podczas zdarzeń transgranicznych (budowa systemu i przekazanie praw państwom ościennym – budowa prototypu w relacjach z republiką czeską).
- aplikacji do monitoringu zasobów Magazynu Centralnego KG PSP, racji żywnościowych i plandek.
- aplikacji do szeroko rozumianego monitoringu Ratownictwa Medycznego w PSP w szczególności:
  - wypełniania Indywidualnej Karty Ratownika Medycznego oraz karty Udzielonej Kwalifikowanej Pierwszej Pomocy (gromadzenie zbieranych danych oraz ich analiza),
  - wykształcenia ratowników medycznych w KSRG, doskonalenia zawodowego z KPP strażaków KSRG, w tym szkoleń i egzaminów potwierdzających z zakresu kwalifikowanej pierwszej pomocy (kurs/ egzamin),
  - stanu osobowego i wykorzystania planowanych do wprowadzenia Zespołów Wsparcia Medycznego KSRG (gromadzenie zbieranych danych oraz ich analiza).
  - aplikacji do samodiagnozy i profilaktyki problemów/trudności psychologicznych strażaka.
- aplikacji uruchamianej ad hoc do wykorzystania podczas zjawisk pogodowych, w szczególności dot. burz silnych wiatrów, podtopień i powodzi, umożliwiającej monitorowanie on-line interwencji PSP i OSP ze szczególnym uwzględnieniem:
  - liczby interwencji od początku zjawiska pogodowego,

- liczby osób zabitych i rannych, w podziale na osoby cywilne i ratowników,
- liczby uszkodzonych budynków mieszkalnych i gospodarczych, w tym zerwanych da-chów, uszkodzonych dachów i innych uszkodzeń,
- budynków, wobec których KDR wydał zalecenie o ich nieużytkowaniu,
- podtopień: budynków, dróg,
- itp.

- narzędzi teleinformatycznych (platform low-code do budowania aplikacji bez kodowania) pozwalających na digitalizowanie procesów i tworzenie ad hoc aplikacji do monitoringu innych zasobów, jak np.
  - podczas rozpoczętej przez Federację Rosyjską wojny na Ukrainie i konieczności posiadania w stanowiskach kierowania PSP nt. wykorzystania autokarów innych służb i instytucji oraz przewoźników prywatnych wspomagających PSP celem przemieszczania ludzi z granicy RP w głąb kraju,
  - miejsc doraźnego schronienia,
  - potrzeb dot. zagrożenia na rzece Odra
  - itp.
- narzędzi teleinformatycznych usprawniających obieg informacji na potrzeby międzynarodowego punktu kontaktowego, jakim jest stanowisko kierowania Komendanta Głównego PSP, pod kątem międzynarodowych działań ratowniczych i humanitarnych.
- spójnego środowiska, w tym mapowego do wspomagania zarządzania działania ratowniczymi na terenie kraju jak i poza jego granicami (tzw. moduł dla pracy sztabu), dzięki któremu wszyscy uczestnicy, ze szczególny uwzględnieniem korpusu dowódczego będą mieć możliwość interakcji zarówno między sobą jak i ze sztabem, a na mapie udostępnione zostaną dane istotne z punktu widzenia prowadzenia działań, w szczególności informacje na temat:
  - obszarów zagrożonych,
  - podziału terenu działań na rejony operacyjne (odcinki bojowe),
  - danych zebranych podczas inwentaryzacji przez użytkowników mobilnych,
  - danych na temat ewidencji SiS: w działaniach, w dojeździe, na obozowisku (PPSiS),
  - organizacji łączności i przydziału odpowiednich sieci radiowych.

- jednolitego systemu wideokonferencyjnego w całym kraju, ze szczególnym uwzględnieniem przekaz obrazu z miejsca działań ratowniczo-gaśniczych do stanowisk kierowania PSP on-line.
- przestrzeni do składowania dokumentacji stanowisk kierowania PSP wszystkich szczebli, umożliwiającej aktualizacje dokumentów, w tym opracowanie: zbioru dokumentacji SK PSP ze szczególnym uwzględnieniem: zasad, instrukcji, metodyk wdrażanych przez Komendanta Głównego PSP, opisanych w Rozdziale 2 Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 17 września 2021 r. w sprawie szczegółowej organizacji krajowego systemu ratowniczo-gaśniczego, pn. funkcjonowanie ksrg na obszarze powiatu, województwa i kraju, w sposób scentralizowany.
- narzędzi teleinformatycznych pozwalających na generowanie raportów, zestawień i analiz, ze szczególnym uwzględnieniem raportów z codziennych statystyk dot. liczby zdarzeń:
  - współpracy z PRM, w tym wykonywaniu zadań z zakresu kwalifikowanej pierwszej pomocy w stosunku do poszkodowanych do czasu przybycia ZRM,
  - współpracy z LPR, w tym zabezpieczaniu lądowisk,
  - współpracy z Policją: w tym wspólnych patroli,
  - osób rannych i śmiertelnych w tlenku węgla,
  - utonięć.
- narzędzi teleinformatycznych usprawniających funkcjonowanie stanowisk kierowania PSP wszystkich szczebli [SK KG PSP, SK KW PSP, SK KP (KM) PSP] w miejscach zastępczych, wraz z utrzymaniem ich kluczowych funkcjonalności zapewniających realizację zadań opisanych w Rozdziale 10 Rozporządzenia Ministra Spraw Wewnętrznych I Administracji z dnia 17 września 2021 r. w sprawie szczegółowej organizacji krajowego systemu ratowniczo-gaśniczego, pn. Organizacja stanowisk kierowania.

Cel II – budowa systemów łączności i migracja z usług analogowych do cyfrowych.

Obecnie jednostki ochrony przeciwpożarowej prowadzą korespondencję radiową głównie w trybie analogowym zarówno na kanałach otwartych jak i zamkniętych (poprzez kod CTCSS) w paśmie VHF. Dodatkowo w czterech miastach tj. Krakowie, Łodzi, Szczecinie i Warszawie, Państwowa Straż Pożarna wykorzystuje systemy trankingowe (TETRA), których dysponentem jest Policja. W związku z powyższym Państwowa Straż Pożarna dla realizacji łączności radiowej wykorzystuje obecnie częstotliwości z pasma UKF

136-174 MHz (w modulacji F3E oraz FXD FXE), będącego w dyspozycji resortu spraw wewnętrznych. Ponadto PSP jest również na etapie wdrażania usług z pasma TETRA 380-400 MHz.

Radiowe systemy łączności na potrzeby PSP i OSP obsługiwane są przez kilkanaście merytorycznych osób w kraju, ale pomimo braków kadrowych i finansowych systemy radiowe są rozwijane i utrzymywane.

Kierując się wymaganiami technicznymi i optymalnym wykorzystaniem przydzielonego pasma częstotliwości zorganizowano grupy kanałów tworząc sieci radiowe o określonym przeznaczeniu. Ze względu na obszar pracy wyróżnia się następujące sieci:

- sieć stałą,
- sieć ruchomą o stałym obszarze pracy,
- sieć ruchomą o zmiennym obszarze pracy.

Jednostki ochrony przeciwpożarowej w zależności od poziomu hierarchii, struktury, poziomu dowodzenia, wykorzystują odpowiednie sieci tak, aby zapewniona była komunikacja pomiędzy poszczególnymi szczeblami kierowania działaniami ratowniczymi, począwszy od poziomu interwencyjnego poprzez taktyczny, a kończąc na strategicznym.

Mając na uwadze, przede wszystkim konieczność zapewnienia w Państwowej Straży Pożarnej szyfrowania sygnału, ze szczególnym uwzględnieniem zdarzeń w ramach, których następuje styczność z informacjami wrażliwymi, ale również wydajność widmową, koniecznym staje się uruchomienie usług i transmisji cyfrowych pozwalających na zdecydowanie bliższe niż w sieciach analogowych umieszczanie kanałów częstotliwościowych, bez konieczności zapewnienia szerokich przerw między nimi, a także pozbycia się zakłóceń pomiędzy stronami wymiany korespondencji.

Celem staje się budowa systemu oparta na technologiach radiokomunikacyjnych, mających potencjał do budowy wielkoobszarowych cyfrowych systemów łączności radiowej w świetle priorytetów służby w zakresie niezbędnych usług, a także rekomendacji kierunkowej do wdrożenia CSR w Państwowej Straży Pożarnej. Podczas budowy takiego systemu należałoby także uwzględnić jego kompatybilność dla potrzeb organów i jednostek organizacyjnych podległych ministrowi właściwemu do spraw wewnętrznych lub przez niego nadzorowanych z określeniem możliwości udostępnienia zasobów CSR innym użytkownikom, realizującym zadania z obszaru bezpieczeństwa i porządku publicznego lub ratownictwa oraz zarządzania kryzysowego.

Oceniając i analizując eksploatowane/rozwijane w Polsce rozwiązania dotyczące łączności cyfrowej najbardziej optymalnym-technologicznym wyborem w zakresie łączności mobilnej dla potrzeb Państwowej Straży Pożarnej na obecną chwilę jest system standardu TETRA. Dotyczy to aspektów: dostępności szerokiej gamy urządzeń, bezpieczeństwa, niezawodności, sprawności przekazywania komunikatów głosowych, dynamicznej aranżacji zasobów systemowych.

TETRA (TErrestial Trunked RAadio) jest cyfrowym, trankingowym standardem radiokomunikacyjnym stworzonym przez Europejski Instytut Standardów Telekomunikacyjnych (ETSI) dla potrzeb łączności PMR różnych grup użytkowników, w szczególności tych z obszaru bezpieczeństwa i ratownictwa. Oferuje skalowalną architekturę, umożliwiającą budowę systemów różnej wielkości, włącznie z systemami ogólnokrajowymi. Już w 2003 roku system TETRA został wymieniony w dokumencie Police Co-Operation Recomendations and Best Practices (Volume 4) - June 2003, referującym do artykułu 44 Konwencji Wykonawczej do Układu z Schengen z dnia 14 czerwca 1985 roku, jako system rekomendowany do stosowania w obszarze Schengen.

Ze względu na swoje przeznaczenie, standard TETRA oferuje użytkownikom specyficzne właściwości, w tym:

- krótki czas zestawiania połączeń abonenckich (poniżej 0,5 sek.);
- bezpieczne mechanizmy szyfrowania korespondencji w interfejsie powietrznym, działające w oparciu o dedykowane algorytmy szyfrowania;
- mechanizmy autentykacji użytkowników i opcjonalnie infrastruktury systemowej;
- realizację wywołań alarmowych bez względu na stopień zajętości systemu;
- realizację dupleksowych połączeń telefonicznych;
- możliwość realizowania połączeń w trybie bezpośrednim (DMO, ang. Direct Mode Operation), bez wykorzystywania infrastruktury stałej systemu, przy zachowaniu szyfrowania korespondencji kluczami SCK.

Standard oferuje również szereg innych funkcjonalności, istotnych z punktu widzenia użytkowników segmentu bezpieczeństwa i ratownictwa, jak np.:

- połączenia grupowe;
- połączenia indywidualne (simpleksowe i dupleksowe);
- przesyłanie krótkich wiadomości (usługa SDS) i statusów;
- pakietową transmisję danych;
- identyfikację abonenta;

- dynamiczne dostosowywanie obsady grupowej terminali (DGNA);
- mechanizmy kolejkowania i priorytetyzacji użytkowników.

W standardzie TETRA ujęto szereg funkcjonalności i mechanizmów zwiększających bezpieczeństwo korespondencji i danych. Do podstawowych należą:

- Mechanizm autentykacji terminali przez infrastrukturę systemu TETRA i infrastruktury przez terminale;
- Mechanizm wymiany kluczy szyfrujących w terminalach poprzez interfejs powietrzny (OTAR, ang. Over The Air Re-keying);
- Mechanizm zdalnego blokowania / odblokowywania terminali abonenckich (stałego lub tymczasowego);
- Dedykowany zestaw algorytmów TEA (ang. TETRA Encryption Algorithm) dla szyfrowania transmisji w interfejsie radiowym (AIE, ang. Air Interface Encryption), w tym zastrzeżenie algorytmu TEA2 do wykorzystywania przez organizacje rządowe (głównie z obszaru bezpieczeństwa) w państwach Schengen i Unii Europejskiej . Dostęp użytkowników do urządzeń abonenckich wykorzystujących algorytmy TEA jest objęty procedurą licencjonowania;
- Zdefiniowanie klas bezpieczeństwa, powiązanych z różnym stopniem wymagań w zakresie OTAR, szyfrowania (w tym powiązanych z klasą zestawów używanych kluczy AiE oraz ich czasu życia), autentykacji i blokowania możliwości pracy wybranych terminali abonenckich;
- Możliwość dodatkowego szyfrowania informacji pomiędzy użytkownikami końcowymi (E2EE, ang. End To End Encryption), niezależne od szyfrowania AIE.

Ponadto dla niektórych użytkowników TETRA system ten powinien być uzupełniany rozwiązaniem zapewniającym szerokopasmową transmisję danych do przekazywania treści multimedialnych. Z tego powodu policyjny system TETRA powinien być rozpatrywany, jako baza do dalszej rozbudowy w kierunku CSR i należy zadbać o stworzenie ram i mechanizmów finansowania jego rozbudowy i utrzymania.

Pozostałe rozwiązania w sieciach analogowej łączności radiowej i analogowej łączności radiowej w systemie trunckingowym EDACS, nie są odporne na podsłuch lub ingerencję podmiotów i osób nieupoważnionych. Z tego powodu sieci analogowej łączności radiowej i EDACS nie powinny być brane pod uwagę, jako baza do rozbudowy w kierunku CSR.

Również rozwiązania DMR nie są perspektywiczne, jako baza do rozbudowy w kierunku CSR z wielu powodów, m.in:

- brak istotnych wdrożeń w Europie dla służb bezpieczeństwa porządku publicznego,
- brak możliwości zaawansowanej integracji z systemami państw sąsiadujących,
- brak dostępnych częstotliwości,
- brak wdrożeń wielkoskalowych na świecie (systemy krajowe, z co najmniej kilkudziesięcioma tysiącami terminali i stacjami bazowymi liczonymi w tysiącach).

DMR (ang. Digital Mobile Radio) to otwarty standard cyfrowej łączności radiowej opracowany przez Europejski Instytut Norm Telekomunikacyjnych (ETSI) i zatwierdzony w 2005 roku. Specyfikacja standardu DMR jest zawarta w serii dokumentów ETSI TS 102 361 (cz. 1-4). Standard DMR umożliwia opracowywanie urządzeń przez różnych producentów wykorzystujących wspólną infrastrukturę, lepsze zarządzanie pasmem częstotliwości a także działanie na wspólnej infrastrukturze radiowej w pasmach VHF. Standard DMR jest standardem otwartym, stworzonym przede wszystkim z myślą o jego zastosowaniu jako rozwiązania biznesowego dla podmiotów gospodarczych np. z sektora transportu, produkcji lub ochrony osobistej, korzystających z pasm licencjonowanych. Budowa i możliwości systemu DMR, predestynuje systemy DMR do zastosowania na obszarach o niezbyt dużej gęstości użytkowników.

Rozwiązanie DMR idealnie wpisuje się jednak w potrzeby Państwowej Straży Pożarnej szczególnie jako sieci ruchome o zmiennym obszarze pracy przewidziane dla potrzeb kanałów:

- Dowodzenia i Współdziałania uruchamianych doraźnie podczas akcji ratowniczo gaśniczych oraz ćwiczeń, służących zapewnieniu łączności dowodzenia i współdziałania pomiędzy siłami ratowniczymi własnymi oraz współdziałającymi.
- Ratowniczo-Gaśniczych przeznaczonych dla potrzeb łączności w miejscu prowadzenia akcji ratowniczo gaśniczej.

Główną ideą staję się w tym miejscu stworzenie jednolitego cyfrowego systemu radiokomunikacyjnego zapewniającego komunikację na potrzeby realizacji zadań z zakresu bezpieczeństwa Państwa, ochrony porządku publicznego, ochrony ludności oraz zarządzania kryzysowego, który realizowałby również funkcje pomocnicze (uzupełniające) w stosunku do systemów związanych z obronnością kraju. Celem głównym przedmiotowego projektu jest objęcie systemem cyfrowej łączności radiowej całego obszaru kraju z jego wykorzystaniem przez służby porządku publicznego oraz bezpieczeństwa wewnętrznego takie jak: Policję, SG, ABW, CBA, SOP oraz PSP. Jest to zgodne ze standard TETRA, którego jedną z cech jest skalowalność, polegająca na możliwości kształtowania

systemu w zakresie struktury elementów składowych oraz ich liczby. Pozwala to na etapową rozbudowę systemu w ujęciu terytorialnym (zasięgi) i liczby (pojemność) oraz rodzajów użytkowników (rodzaje usług), aż do systemu ogólnokrajowego, wykorzystywanego przez różne służby i organizacje. Organizacja zarządzania systemem oparta o stworzenie wewnętrznych sieci wirtualnych (agencji), połączona z systemem nadawania uprawnień administratorom każdej z tych sieci pozwala na stworzenie logicznie niezależnych systemów łączności z jednoczesną możliwością ich pełnej współpracy na platformie jednego systemu. Pozwala to zachować odrębność systemów wewnętrznej łączności każdej z organizacji korzystających z systemu, ale jednocześnie oferuje bardzo łatwą organizację współdziałania pomiędzy nimi, gwarantując pełną zgodność technologiczną.

Wdrożenie nowoczesnych rozwiązań radiowych w Państwowej Straży Pożarnej pozwoli na poprawę efektywności działań i skuteczniejszą ochronę ludzi i mienia. Opracowanie koncepcji i minimalnych wymagań techniczno-funkcjonalnych dla radiowych systemów alarmowania jednostek Ochotniczych Straży Pożarnych, które są strategiczną częścią Krajowego Systemu Ratowniczo-Gaśniczego przyczynią się do lepszej koordynacji działań oraz szybszej reakcji na zagrożenia. Należy również zwrócić uwagę, że Państwowa Straż Pożarna i Ochotnicze Straże Pożarne oraz inne jednostki ochrony przeciwpożarowej np. Wojskowa Ochrona Przeciwpożarowa to organizacje wzajemnie się przenikające i współdziałające w ramach Krajowego Systemu Ratowniczo Gaśniczego. W Polsce według stanu na dzień 2 lutego 2023 r. funkcjonuje 15 986 Ochotniczych Straży Pożarnych, z czego 4 868 jest włączonych do KSRG. Jednym z warunków włączenia jednostki OSP do KSRG jest posiadanie skutecznego systemu alarmowania jednostki do działań. Przepisami określającymi włączenie jednostek OSP do KSRG jest Rozporządzenie Ministra Spraw Wewnętrznych z dnia 15 września 2014 r. w sprawie zakresu, szczegółowych warunków i trybu włączania jednostek ochrony przeciwpożarowej do krajowego systemu ratowniczo-gaśniczego do systemu KSRG. Zgodnie z § 2. ust. 1. pkt. 1 lit. c) i d) włączana jednostka powinna posiadać m.in. skuteczny system łączności powiadamiania i alarmowania oraz urządzenia łączności w sieci radiowej systemu na potrzeby działań ratowniczych. Ponadto, zgodnie z wytycznymi Komendanta Głównego Państwowej Straży Pożarnej za skuteczny system powiadamiania i alarmowania należy uznać system posiadający przymioty usługi gwarantowanej, umożliwiając bieżącą kontrolę stanu działania usługi. Za taki uznaje się system selektywnego alarmowania, który stanowi podstawowy element powia-

damiania i alarmowania jednostek do działań. Inne dostępne rozwiązania np. powiadamianie przez GSM, stanowią uzupełnienie podstawowego sposobu alarmowania.

Cel III – budowa nowego scentralizowanego systemu wspomagania decyzji państwowej straży pożarnej (SWD PSP).

Fundamentalnym zadaniem systemu SWD PSP jest wspomaganie pracy strażaków na każdym z poziomów kierowania, ze szczególnym uwzględnieniem stanowisk kierowania PSP, w tym: wymiany informacji z Centrami Powiadamiania Ratunkowego, dyspozytorniami PRM oraz stanowiskami kierowania Policji, a także dysponowanie sił i środków jednostek ochrony przeciwpożarowej do działań.

Mając na uwadze kluczowość tego systemu dla procesów operacyjnych zachodzących w PSP niezbędnym jest, również, aby system ten na bieżąco był monitorowany utrzymywany na odpowiednim poziomie z zachowaniem określonego SLA - gwarancji świadczenia usług – Service Level Agreement, rozbudowywany i modyfikowany.

Zgodnie z obowiązującym stanem prawnym tj. Ustawą z dnia 24 sierpnia 1991 r. o ochronie przeciwpożarowej za zapewnienie funkcjonowania SWD PSP, stanowiącego system teleinformatyczny wspierający wykonywanie zadań krajowego systemu ratowniczo-gaśniczego przez jednostki organizacyjne Państwowej Straży Pożarnej oraz przyjmowanie zgłoszeń alarmowych z centrów powiadamiania ratunkowego, o których mowa w ustawie z dnia 22 listopada 2013 r. o systemie powiadamiania ratunkowego odpowiada Komendant Główny Państwowej Straży Pożarnej.

W chwili obecnej system SWD PSP ma postać rozproszoną na 335 instancji poziomu powiatowego, 16 instancji poziomu wojewódzkiego oraz 1 instancję centralną, co negatywnie wpływa na jego codzienne utrzymanie i modernizację, a każda zmian musi być wprowadzana oddzielnie we wszystkich wyżej wymienionych jednostkach. Ponadto technicznie i technologicznie produkt jest odbiegającym od podobnych systemów funkcjonujących w Państwie.

Wypełnia on co prawda wszystkie opisane prawnie zapisy i instrumenty, jednak na chwile obecną systemem SWD PSP jest produktem służącym strażakom do ewidencjonowania, niż wspomagania dyżurnych i dyspozytorów stanowisk kierowania, funkcjonariuszy pracujących w sztabach, szczególnie w przypadku uruchamiania wielkoobszarowych działań ratowniczych i kierowania poziomu taktycznego czy strategicznego oraz kierujących działaniem ratowniczym od najmniejszych zdarzeń poczynając.

Taki system zupełnie nie wpisuje się w potrzeby XXI wieku oraz w opisywany proces cyfryzacji Państwowej Straży Pożarnej.

Należy dążyć do budowy i wdrożenia nowego systemu SWD PSP, gdzie w ramach realizowanego przedsięwzięcia zmieniona powinna zostać architektura systemu z rozproszonej na scentralizowaną, co usprawni procesy obsługi zdarzeń oraz umożliwi łatwiejszą integrację z zewnętrznymi systemami teleinformatycznymi, w tym właśnie w szczególności z systemem powiadamiania ratunkowego.

Zgodnie z postawionymi wymaganiami funkcjonalnymi do budowy nowego SWD PSP system ten powinien obsługiwać przyjęcie zgłoszeń i rejestrację zdarzeń zgodnie z obowiązującym stanem prawnym oraz posiadać inne funkcje takie jak:

1) alarmowanie i powiadamianie sił i środków ksrg oraz innych SiS,
2) dysponowanie sił i środków ksrg oraz innych SiS do działań ratowniczych,
3) nadzorowanie i koordynowanie działań ratowniczych,
4) sporządzanie dokumentacji z prowadzonych działań operacyjnych,
5) wymianę informacji i danych między wszystkimi jednostkami organizacyjnymi Państwowej Straży Pożarnej oraz innymi (CPR, OSP, inne JOP, Policja, PRM, itd.),
6) prowadzenie ewidencji podmiotów, sił i środków Państwowej Straży Pożarnej, Ochotniczej Straży Pożarnej, Zakładowych Straży Pożarnych i Zakładowych Służb Ratowniczych, WSP, innych jednostek i podmiotów współpracujących,
7) prowadzenie ewidencji dostępnych dla Państwowej Straży Pożarnej sił i środków innych zasobów pochodzących z instytucji i organizacji współpracujących z Państwową Strażą Pożarną, ksrg oraz innymi JOP,
8) współpracę z urządzeniami łączności oraz urządzeniami umożliwiającymi śledzenie pojazdów, nadzór, alarmowanie i powiadamianie sił i środków ksrg, a także sterowanie automatyką przemysłową wykorzystywaną w jednostkach organizacyjnych Państwowej Straży Pożarnej oraz Ochotniczej Straży Pożarnej i innych JOP,
9) generowanie analiz, raportów, zestawień i statystyk na podstawie wszystkich danych wprowadzonych do systemu,
10) pozyskiwanie danych przestrzennych udostępnianych za pośrednictwem systemu, o którym mowa w art. 40 ust. 3e ustawy z dnia 17 maja 1989 r. – Prawo geodezyjne i kartograficzne (Dz. U. z 2010 r. Nr 193, poz. 1287, późn. zm.), z Głównego Urzędu Geodezji i Kartografii,

11) korzystanie z usług danych przestrzennych, udostępnionych za pośrednictwem systemu, o którym mowa w art. 40 ust. 3e ustawy z dnia 17 maja 1989 r. – Prawo geodezyjne i kartograficzne, z Głównego Urzędu Geodezji i Kartografii,
12) wymianę informacji z CPR za pośrednictwem interfejsu komunikacyjnego, o którym mowa w art. 13 ust. 2 ustawy o systemie powiadamiania ratunkowego,
13) pozyskiwanie i prezentację danych dotyczących lokalizacji zakończenia sieci, z którego zostało wykonane połączenie do numeru alarmowego, oraz danych dotyczących abonenta, o których mowa w art. 78 ust. 2 ustawy – Prawo telekomunikacyjne, za pośrednictwem centralnego punktu systemu centrów powiadamiania ratunkowego, o którym mowa w art. 78 ust. 4 pkt 1 ustawy – Prawo telekomunikacyjne, lub przekazanych z centrum
14) możliwość współpracy z innymi systemami teleinformatycznymi za pośrednictwem interfejsów zrealizowanych w architekturze otwartej np. CEPIK, PESEL, SWD Policji, SWD PRM.

Bardzo ważną nową funkcjonalnością budowanego system SWD PSP powinno być posiadanie przez niego budowy modułowej, gdzie wszystkie moduły będą dostępne i uruchamiane z jednego głównego interfejsu po jednokrotnej autoryzacji do systemu.
Tymi modułami powinny być:

1. Moduł Wspomagania Decyzji:

Moduł zawierający powiązane ze sobą logicznie podpowiedzi do dysponowania SiS na podstawie planów operacyjnych, analiz, zasad (w tym przede wszystkim zasad dysponowania, które wskazują na zgodność zadysponowanych SiS z wytycznymi określonymi przez Komendanta Głównego PSP oraz zasadami opracowanymi w jednostce macierzystej. Podpowiedzi będą uzależnione od lokalizacji miejsca zdarzenia oraz lokalizacji SiS, rodzaju i podrodzaju zdarzenia, informacji w Karcie Zdarzenia (słowa klucze) oraz od zarządzanego administracyjnie zestawu innych zdefiniowanych na potrzeby danej jednostki pól oraz dokumentów. Wszystkie dane będą widoczne na mapie wraz z uwzględnieniem współrzędnych jednostek ochrony przeciwpożarowej, SiS na podstawie danych z AVL (automatic vehicle location) oraz obszarów chronionych dla JOP i SGR. Komponent lokalizacji pojazdów pożarniczych na mapie AVL niezbędny jest podczas działań na terenie kraju, co szczególnie jest ważne w przypadku angażowania sił i środków z wielu województw oraz umożliwi lokalizowanie pojazdów pożarniczych podczas działań międzynarodowych, co w chwili obecnej jest nie możliwe. System dzięki możliwościom nieograni-

czonej rozbudowy będzie posiadał podstawy do uruchomienia rozwiązań na miarę XXI wieku, w tym pod kątem bieżącego ewidencjonowania sił i środków przez KDR, w szczególności:

- dojeżdżających do Punktu Przyjęcia Sił i Środków (PPSiŚ),
- zaewidencjonowanych w PPSiŚ,
- dojeżdżających do Sztabu/KDR,
- będących na odcinkach bojowych i/lub organizujących zaopatrzenie wodne.

Dodatkowo w powiązaniu z modułem Operacyjnego Katalogu Obiektów (OKO) widoczne będą dane dot. obiektów oraz dane historyczne zawarte w SWD PSP – np. zdarzenia, które już były pod tym samym adresem. W module będzie też istnieć funkcjonalność powiadamiania o zdarzeniach długotrwałych, konieczności utworzenia Informacji ze Zdarzenia (IzZ), zbliżających się terminach przeglądów, badań, kalibracji itp.

2. Moduł Operacyjnego Katalogu Obiektów (OKO)

Wymagania modułu Operacyjnego Katalogu Obiektów mają na celu stworzenie bazy danych o budynkach, obiektach i kompleksach stanowiących istotne zagrożenie dla bezpieczeństwa. Moduł umożliwi dodawanie, edytowanie, wyszukiwanie informacji o ww. obiektach i kompleksach po wszystkich polach (również generycznych). Moduł z zasady przechowywać będzie dane istotne z punktu widzenia prowadzenia działań m.in.: lokalizację, dostęp do budynku, dane administratora, dane techniczne, urządzenia ppoż., monitoring ppoż., zaopatrzenie wodne, dane dot. ewakuacji, dane o zagrożeniach i inne. Umożliwi również dostęp do dokumentacji obiektu/kompleksu: planów ewakuacyjnych, planów zabezpieczenia i innych. Możliwy będzie import i aktualizację wybranych danych i dokumentów z Cyfrowej Książki Obiektu Budowlanego prowadzonej przez GUNB. Dane prezentowane będą w formie karty obiektu/kompleksu lub skróconej karty obiektu. System automatycznie łączy kartę zdarzenia z kartą obiektu/kompleksu. Pozwala także na dostęp do karty obiektu/kompleksu w aplikacji mobilnej. Dane z modułu zasilają moduł raportowy i umożliwiają przygotowanie dedykowanych raportów. Dane w aplikacji wypełniane są w dwóch trybach: operacyjnym i prewencyjnym. W trybie operacyjnym wybrane pola karty wypełniane są po przeprowadzonych działaniach lub podczas rozpoznania operacyjnego obiektu przez funkcjonariusza z pionu operacyjnego. Tryb obejmuje Tryb prewencyjny obejmuje wszystkie pola wypełniane przez funkcjonariusza z pionu prewencyjnego podczas czynności kontrolno-rozpoznawczych. System flaguje odpowiednio tryb wypełnienia w sposób widoczny dla użytkownika.

3. Moduł OSP

Moduł dla Ochotniczych Straży Pożarnych będzie służył do przekazywania danych o zgłoszeniach i zdarzeniach dla strażaków OSP oraz będzie bazą danych dot. jednostki OSP wraz z SiS, zarządzanym przez daną OSP. Rozwiąże to konieczność wprowadzania danych do SWD PSP jedynie przez PSP, wymagać będzie jednak potwierdzenia poprawności wprowadzenia danych przez uprawnionego funkcjonariusza PSP. W PSP dane pojawiać się będą w systemie zaraz po wprowadzeniu ich przez OSP i zatwierdzone przez pion operacyjny z właściwego miejscowo powiatu. Ponadto strażacy OSP oprócz danych dot. zdarzeń będą mieli dostęp do swoich statystyk, ewentualnie do statystyk dot. całej gminy lub powiatu. Dane wprowadzone przez OSP będą pozwalały na określenie gotowości operacyjnej jednostki na daną chwilę na postawie wprowadzonych badań, szkoleń, wieku oraz stanu pojazdów i sprzętu. Dodatkowo będzie również funkcjonowała aplikacja mobilna (na telefon komórkowy), która pozwoli na określenie dostępności sił w danej chwili. Dostęp do modułu dla jednostek Ochotniczych Straży Pożarnych będzie nieodpłatny i innowacyjny na rynku systemów wspomagających działania ratownicze Ochotniczych Straży Pożarnych w szczególności będzie umożliwiał:

- monitorowanie przez SK PSP gotowości OSP i ich członków;
- podpowiadanie dyżurnemu w stanowiskach kierowania PSP obszarów chronionych oraz SIS dysponowanych do konkretnego rodzaju zdarzenia - generowanie obszarów chronionych w tym na podstawie gotowości OSP;
- prezentowanie aktualnego statusu OSP: w podziale, wycofany, w służbie, w akcji, udział w ćwiczeniach, itp.;
- w razie braku wyjazdu zadysponowanej do zdarzenia jednostki OSP, po zadanym czasie automatycznie będzie generowanie informacji o braku wyjazdu z numerem karty zdarzenia. Dodatkowo w systemie będzie funkcjonalność generowania dedykowanego zestawienie z informacją o jednostce, która nie wyjechała z możliwością ustawienia rankingu jednostek OSP najczęściej niewyjeżdżających do działań (z informacją o przynależności jednostki do ksrg). Ponadto system będzie wymuszał podanie przyczyny braku wyjazdu wg zdefiniowanego katalogu przyczyn braku wyjazdu OSP. Do braku wyjazdu nie będzie się zaliczało SiS zawróconych z trasy lub SiS, które zadysponowano do zdarzenia, a następnie anulowanego. Informacja ta będzie podpinana do IzZ.;

- automatyczne zdejmowanie ze stanu środka pianotwórczego, sorbentu i neutralizatora w przypadku jednostek OSP;
- na podstawie historycznych danych podpowiadanie przy dysponowaniu OSP w tablicy gotowości operacyjnej i na mapie średni czas wyjazdu danej OSP (czas od zadysponowania do wyjazdu);
- uruchomienie warstwy, ikony z danymi dotyczącymi OSP w zakresie: poziomu dyspozycyjności w poprzednich latach, wyposażenia w samochody i wybrany sprzęt: np. hydraulika;
- uzupełnianie danych w systemie przez użytkowników z OSP
- łączenie się użytkowników z OSP z aplikacja poprzez logowanie za pomocą nazwy użytkownika i hasła;
- uzupełnianie przez użytkowników z OSP w systemie danych dotyczące SiS jednostki OSP oraz gotowość ratowników;
- tworzenie przez użytkowników z OSP szkicu Informacji ze zdarzenia IzZ;
- automatyczne potwierdzenie udziału ratowników OSP w działaniach do wypłaty ekwiwalentu;
- dostęp do modułu mapy, z widocznością SiS przy danym zdarzeniu.

4. Moduł zarządzania rolami i uprawnieniami

Rozbudowany, w miarę możliwości, aż do najmniejszego pola (obiektu) system zarządzania dostępnością do danych – by uniemożliwić osobom niepowołanym dostęp do danych, w szczególności w odniesieniu do RODO. Zachowanie widoczności danych w dół, tj. KG widzi dane kraju, KW – swojego województwa, a powiat – swojego powiatu (z możliwością tzw. zaprzyjaźniania, czyli udostępniania wglądu do danych swojej jednostki). Ponadto uprawniania administracyjne do zarządzania systemem powinny być wyodrębnione od podglądu do danych osobowych.

5. Moduł Informacji ze Zdarzenia (IzZ) z możliwością rozbudowy pól, Karty Zdarzenia (KZ), generowanie załączników do rozporządzenia w sprawie szczegółowej organizacji ksrg.

Rozbudowa modułu IzZ jest konieczna z uwagi na zapisy ustawowe (rozporządzenie o ksrg), jak również zachowania danych historycznych do wieloletnich porównań. Dodawanie pól (generyczne, ad hoc) w miarę potrzeb, w miarę możliwości z rozbudowanymi i zdefiniowanymi katalogami z odpowiedziami (eliminowanie pól tekstowych). Główne punkty IzZ rozwijane tylko w przypadku zaznaczenia głównej gałęzi, a zamknięte, gdy

zdarzenie nie dotyczy danej gałęzi danych (wpływ na szybsze wypełnienie IzZ). Moduł powinien zostać wyposażony w sprawdzenie wstępne poprawności wprowadzonych danych poprzez walidację poszczególnych pól, jak również walidację pól w zależności od rodzaju zdarzenia. Każde pole będzie miało możliwość włączenia i wyłączenia podpowiedzi z zasad ewidencjonowania zdarzeń dot. danego pola. Na podstawie danych z IzZ, KZ, będzie możliwość wypełnienia i wydrukowania również innych załączników z rozporządzenia w sprawie szczegółowej organizacji ksrg.

6. Moduł Siły i środki (w tym odwody operacyjne)

Moduł będzie bazą danych ludzi i sprzętu z podziałem na poszczególne JOP oraz ich rodzaje. Skatalogowany zostanie system podpowiedzi danych dla poszczególnych rodzajów pojazdów, sprzętu, ludzi. Spełniona zostanie możliwość dodawania atrybutów, tworzenia grup, zespołów, itp., a także możliwość zakładania walidacji i wyróżniania danych przez system, które wymagają poprawy, wprowadzenia dodatkowych danych lub uzupełnienia np. przeterminowanej daty badań. SiS mają posiadać historię zmian, również przeniesioną z systemu obecnie funkcjonującego. Oprócz pogrupowania SiS i wprowadzenia danych w polach (również generyczne dodawanie) będzie możliwość dodawania atrybutów, które będą również brały udział w module wspomagania decyzji przy dysponowaniu.

7. Moduł mapowy

Tworzyć go będzie mapa powiązana ze wszystkimi danymi w systemie, którym można przyporządkować współrzędne. Powiązana z Siłami i Środkami, OKO oraz modułem Wspomagania Decyzji i modułem analityczno-statystycznym. Możliwość dysponowania z okna mapy oraz podglądu JOP i SiS wraz z określeniem atrybutów (parametrów) do wyświetlenia.

8. Moduł analityczno-statystyczny

Wykorzystanie narzędzia Power BI z zachowaniem podglądu danych w zależności od uprawnień użytkownika i jego jednostki (podgląd krajowy, wojewódzki, powiatowy).

9. Moduł rozliczalności czasów operacyjnych

Moduł umożliwiający na podstawie wprowadzonych do systemu czasów operacyjnych, w tym czasu służby, udziału w zdarzeniach - rozliczalność czasu (w tym dodatek szkodliwy, 1%,).

10. Monitoring SGR oraz modułów

Na podstawie danych z innych systemów i podsystemów (dzięki wdrożeniu narzędzi w chmurze obliczeniowej PSP), w tym module będą prezentowane zestawienia gotowości

operacyjnej SGR, modułów, kompanii oraz innych zdefiniowanych oddziałów i pododdziałów z wyświetlaniem na mapie z informacją o deklarowanym i faktycznym poziomie gotowości.

11. Sztab

Moduł sztabowy będzie miał za zadanie uporządkowanie zagadnień związanych z organizacją i funkcjonowaniem sztabu tworzonego na potrzeby działań ratowniczych oraz zapewnienie przestrzegania jednolitych wytycznych w zakresie jego tworzenia przez kierujących działaniem ratowniczym na poszczególnych poziomach kierowania.

Moduł będzie podpowiadał z jakich elementów Sztab ma się składać oraz definiował zadania dla poszczególnych zespołów i osób funkcyjnych wraz z uprawnieniami, jak również zalecane wyposażenie w sprzęt, pojazdy i ludzi.

Dzięki narzędziu, KDR będzie mógł skupić na najistotniejszych działaniach związanych z kierowaniem i taktyką działań ratowniczych.

Moduł w szczególności będzie miał za zadanie wspomaganie pracy: zespołu operacyjnego (OP), zespołu łączności (IT), zespołu logistyki (LOG), zespołu medialnego (MEDIA) pod kątem:

1) analizowania rodzaju zagrożenia oraz prognozowanie jego rozwoju dla ludzi, zwierząt, środowiska lub mienia;
2) szacowania sił i środków niezbędnych do ograniczenia lub likwidacji zagrożenia;
3) wypracowywania taktyki prowadzenia działań ratowniczych;
4) analizowania funkcjonowania łączności na potrzeby kierowania działaniami ratowniczymi;
5) analizowania stanu zabezpieczenia logistycznego;
6) analizowania stanu zabezpieczenia medycznego;
7) analizowania stanu zabezpieczenia sanitarnego, socjalnego i wsparcia psychologicznego;
8) analizowania zużycia środków gaśniczych, pochłaniających, neutralizatorów oraz zniszczenia sprzętu ratowniczego;
9) dokumentowania przebiegu działań ratowniczych;
10) dokumentowania decyzji podjętych przez Szefa sztabu;
11) gromadzenia danych dotyczących udziału sił i środków w działaniach ratowniczych oraz wniosków z pracy sztabu;

12) planowania miejsc na przyjęcie dodatkowych sił i środków oraz wskazanie miejsc do zakwaterowania i odpoczynku ratowników;
13) przygotowania miejsc do współdziałania KDR ze środkami masowego przekazu oraz organami władzy publicznej;
14) planowania czynności dla podmiotów wspomagających działania ratownicze oraz dla wolontariuszy, o których mowa w ustawie z dnia 24 kwietnia 2003 r. o działalności pożytku publicznego i o wolontariacie.

4.2.2 REFERENCYJNA ARCHITEKTURA CYBERBEZPIECZEŃSTWA W PSP.

Państwowa Straż Pożarna jest ważną instytucją odpowiedzialną za ochronę ludzi i mienia przed pożarami oraz innymi zagrożeniami. Aby zapewnić skuteczne działanie, konieczne jest również zabezpieczenie systemów informatycznych przed cyberatakami. W celu wzmocnienia swojej infrastruktury pod kątem szeroko pojętego cyberbezpieczeństwa Państwowa Straż Pożarna niezwłocznie musi zastosować narzędzie służące do filtrowania ruchu sieciowego i blokowanie niepożądanych połączeń typu firewall. Jest to pierwsza linia obrony przed cyberatakami, dlatego też jego zakup jest kluczowy dla zabezpieczenia systemów PSP rozumianych jako całość. Kolejnym krokiem będzie wzmocnienie koordynacji cyberbezpieczeństwa między poszczególnymi narzędziami i infrastrukturami. Dzięki temu, PSP będzie mogła lepiej zarządzać swoimi zasobami i szybciej reagować na zagrożenia. System powinien obejmować stworzenie 3-4 centralnych systemów cyberbezpieczeństwa w Polsce, które połączą wszystkie narzędzia i infrastruktury w jedną spójną całość. Dzięki temu, będzie możliwe lepsze monitorowanie sytuacji i szybsze reagowanie na zagrożenia. Warto podkreślić, że zakup urządzeń typu firewall oraz wzmocnienie koordynacji cyberbezpieczeństwa między narzędziami i infrastrukturami to tylko pierwszy krok w kierunku zwiększenia bezpieczeństwa systemów PSP. Konieczne będą również regularne aktualizacje oprogramowania, szkolenia dla pracowników oraz wprowadzanie nowych rozwiązań z zakresu cyberbezpieczeństwa.

W miejscu tym należy podkreślić jak ważne jest, aby każdy użytkownik systemu znał podstawowe zagadnienia związane z bezpieczeństwem informacji, takie jak modele bezpieczeństwa, rodzaje ataków, zagrożenia, luki w zabezpieczeniach i związane z nimi ryzyko. Wiedza ta jest szczególnie istotna dla administracji publicznej, takiej jak Państwowa Straż Pożarna, która musi dbać o bezpieczeństwo danych i informacji, którymi

dysponuje w swoich systemach. Każdy pracownik powinien posiadać podstawowe informacje i umiejętności z zakresu zarządzania ryzykiem, reagowania na incydenty bezpieczeństwa i obrona przed zagrożeniami. Zrozumienie tych zagadnień pozwoli na skuteczną ochronę danych organizacji i posiadanych przez nią informacji przed nieautoryzowanym dostępem, co w wielu przypadkach uchroni ją przed potencjalnymi szkodami.

Bezpieczeństwo informacji to ochrona zasobów informacyjnych przed różnego rodzaju zagrożeniami, takimi jak ataki na sieć komputerową, klęski żywiołowe, wandalizm czy nieautoryzowane nadużycie. Zabezpieczenie powinno być dostosowane do środowiska i obejmować najbardziej prawdopodobne formy ataku.

Aktywa, które powinny byś zabezpieczone mogą mieć różne formy. Mogą to być przedmioty materialne, takie jak sprzęt komputerowy albo zasoby logiczne, takie jak oprogramowanie, dane czy własność intelektualna. W dzisiejszych środowiskach komputerowych, tego rodzaju zasoby są często co najmniej tak samo wartościowe, a czasami nawet bardziej wartościowe niż przedmioty materialne. W praktyce oznacza to, że musimy chronić nasze dane i systemy przed osobami, które chcą je nadużyć lub nie powinny mieć do nich dostępu. Administracja publiczna, taka jak Państwowa Straż Pożarna, musi szczególnie dbać o bezpieczeństwo informacji i danych, którymi dysponuje, aby zapewnić ich poufność i integralność.

Zwiększając poziom bezpieczeństwa systemu, zwykle obniża się jego produktywność. W administracji publicznej, szczególnie w Państwowej Straży Pożarnej, ważne jest, aby rozważyć równowagę pomiędzy poziomem bezpieczeństwa a produktywnością. Wartość zabezpieczanego elementu powinna być adekwatna do wprowadzanych środków bezpieczeństwa. Niemniej jednak, w niektórych sytuacjach, nawet imponujące środki bezpieczeństwa mogą być niewystarczające. W takim przypadku należy również wziąć pod uwagę potencjalne koszty zastąpienia zasobów w przypadku ich utraty.

Trudno jest dokładnie określić, kiedy środowisko jest bezpieczne. Regularne aktualizowanie systemów, używanie silnych haseł, czy też odłączenie się od internetu, nie zapewniają bezpieczeństwa w każdej sytuacji. Zawsze istnieją sposoby na obejście zabezpieczeń. Z drugiej strony, łatwiej jest określić sytuacje, w których jesteśmy niezabezpieczeni, np. nieinstalowanie aktualizacji i poprawek bezpieczeństwa, używanie słabych haseł, pobieranie programów z słabych haseł, pobieranie programów z nieznanych źródeł, brak aktualizacji oprogramowania, nieodpowiednie ustawienia bezpieczeństwa, nieprawidłowe wykorzystywanie urządzeń mobilnych i innych urządzeń cyfrowych oraz brak wiedzy

o ochronie danych osobowych i prywatności. Wszystko to może prowadzić do niekontrolowanego przepływu informacji i niebezpiecznego naruszenia bezpieczeństwa. W związku z tym, ważne jest, aby administracja publiczna i Państwowa Straż Pożarna korzystały z odpowiednich narzędzi i rozwiązań, aby zabezpieczyć swoje systemy i dane przed takimi zagrożeniami. W ten sposób można zminimalizować ryzyko i zapewnić bezpieczeństwo informacji, a także zachować ciągłość działania i zaufanie obywateli.

Zagrożenia to takie okoliczności, które mają potencjał wyrządzenia szkody. W poprzednim rozdziale omówione zostały różne rodzaje ataków, które mogą spowodować mniejsze lub większe szkody dla zasobów. Należy zaznaczyć, że zagrożenia są zwykle specyficzne dla konkretnych środowisk, szczególnie w dziedzinie bezpieczeństwa informacji. Przykładowo, choć dany wirus może powodować poważne problemy w systemie Windows, to nie będzie miał żadnego wpływu na komputery z systemem Linux.

Informacja jest kluczowym elementem w działalności Państwowej Straży Pożarnej. Szybkość i trafność podejmowania decyzji zależy w dużej mierze od jakości i dostępności informacji. Niestety, brak specjalistów w dziedzinie IT i cyberbezpieczeństwa powoduje, że jest ona jedną z najbardziej narażonych instytucji administracji publicznej na ataki cyberprzestępców i incydenty związane z bezpieczeństwem informacji.

Brak zespołów monitorujących zagrożenia cyberbezpieczeństwa i incydenty na poziomie krajowym, brak jasnych zasad reagowania na wykryte incydenty oraz brak odpowiednich urządzeń do monitorowania i zatrzymywania włamań, powodują, że dane są narażone na nieuprawnione zmiany i wyciek. W takiej sytuacji, inwestycja w technologię jest kluczowa. Chociaż może być droga, to jednak bezpieczeństwo informacji nie ma ceny.

Można porównać koszt jednego samochodu gaśniczego, który wynosi 1,5 mln zł, do szacowanego rocznego kosztu utrzymania cyberbezpieczeństwa w komendzie głównej Państwowej Straży Pożarnej – czy to dużo? Tak i nie.

Warto zauważyć, że w dzisiejszych czasach praktycznie wszystkie dane są przesyłane przez sieci komputerowe, które nie są własnością instytucji. Wymiana danych w większości przypadków odbywa się przez Internet, co dodatkowo zwiększa ryzyko ataków i incydentów.

Podsumowując, brak specjalistów w dziedzinie IT i cyberbezpieczeństwa w Państwowej Straży Pożarnej jest poważnym zagrożeniem dla danych i informacji. Dlatego inwestycja w technologię jest kluczowa, aby zapewnić bezpieczeństwo cybernetyczne. W przypadku, gdy brakuje specjalistów IT, automatyzacja i technologia stają się sprzymierzeńcem. Dla-

tego, nawet jeśli jest to droższe rozwiązanie, warto zainwestować w technologie zabezpieczające systemy, aby zapewnić ciągłość działania i ochronę danych. To pokazuje, jak ważne jest zabezpieczenie danych i jak dużo trzeba w to zainwestować. Informacja jest kluczowa dla pracy i podejmowania właściwych decyzji, a jej nieuprawniona zmiana może prowadzić do błędnych decyzji.

Współczesne środowisko cyfrowe Państwowej Straży Pożarnej wymaga stosowania narzędzi zapewniających elastyczność w dostępie do zasobów i usług przy jednoczesnym zapewnieniu cyberbezpieczeństwa. Środowisko cyfrowe powinno wspierać zarówno stacjonarny, zdalny jak i mobilny model pracy. Co więcej, powinno uwzględniać stosowanie różnych rozwiązań do wytwarzania i konsumpcji treści, a także umożliwiać w ściśle zdefiniowanych warunkach dostęp do zasobów i usług informacyjnych z urządzeń służbowych i prywatnych.

Model bezpieczeństwa dla współczesnego cyfrowego środowiska PSP musi uwzględniać ochronę przed zaawansowanymi atakami ukierunkowanymi na:

- tożsamość,
- dane,
- aplikacje,
- infrastrukturę.

W związku z koniecznością zapewnienia ciągłości działania, zwiększenia elastyczności i umożliwienia pracownikom Państwa Straży Pożarnej wykonywania ich obowiązków nie tylko z siedziby organizacji, ale również poza jej granicami, konieczne jest wprowadzenie rozwiązań umożliwiających im bezpieczną pracę zdalną.

Praca zdalna niesie ze sobą wiele wyzwań zarówno dla Państwa Straży Pożarnej, jak i dla użytkowników końcowych w tej Straży Pożarnej– od rozwiązania problemów związanych ze zdalnym dostępem, aż po bezpieczną współpracę z podmiotami zewnętrznymi.

Pracownicy i funkcjonariusze Państwowej Straży Pożarnej są narażeni na zaawansowane ataki wyspecjalizowanych grup hakerskich (zarówno motywowanych kryminalnie jak i politycznie), coraz częściej sponsorowanych przez rządy państw prowadzących ofensywne działania w cyberprzestrzeni. Właściwe zapewnienie bezpiecznego środowiska pracy zdalnej wymaga spełnienia szeregu wymogów dotyczących między innymi:

- ochrony i zarządzanie tożsamością pracowników, często w sfederalizowanym środowisku,

- ochrony urządzeń służbowych oraz prywatnych z których korzystają użytkownicy, w tym urządzeń typu PC, tabletów i smartfonów,
- wykrywania i blokowania ataków sieciowych i złośliwego oprogramowania dostarczanego najczęściej jako załączniki poczty elektronicznej oraz umieszczanego na stronach internetowych, na które przekierowywany jest nieświadomy zagrożenia użytkownik – największym wyzwaniem dla urzędów Państwowej Straży Pożarnej wciąż pozostaje ochrona przez zagrożeniami typu „zero-day", na które nie ma poprawek bezpieczeństwa,
- zapobiegania przypadkowemu lub świadomemu ujawnianiu informacji.

Państwowa Straż Pożarna w środowisku biurowym wykorzystuje obecnie w większości środowisko MS Windows 10 oraz pakiety biurowe wielu producentów, gdzie wiodącym jest Microsoft Office (MS 365) oraz własne np. utrzymywane przez komendy PSP serwery pocztowe rozwiązania na zasadzie najmu usług, które wykorzystywane są do komunikacji wewnętrznej i zewnętrznej.

Wraz z wprowadzeniem nowych zaawansowanych funkcji i usług integrujących zabezpieczenia na poziomie stacji roboczych (Windows 10), aplikacji biurowych (Office 365/Microsoft 365) oraz zarządzania mobilnością i bezpieczeństwem urządzeń (Enterprise Mobility & Security) pojawiła się możliwość stworzenia w Państwa Straży Pożarnej Referencyjnej Architektury Cyberbezpieczeństwa z wykorzystaniem pakietu Microsoft 365.

Poniżej przedstawione zostały scenariusze i obszary ataków na urzędy administracji publicznej oraz użytkowników pracujących zdalnie i mobilnie oraz sposoby ograniczenia tego typu ataków z wykorzystaniem rozwiązań zintegrowanych w Microsoft 365. Scenariusze te dotyczą zarówno urządzeń firmowych, z których korzysta użytkownik w domu, jak i urządzeń należących do użytkownika, które poza pracą wykorzystywane są do celów prywatnych (BYOD).

- Kradzież tożsamości

Atak typu "Kradzież tożsamości" polega na nieautoryzowanym uzyskaniu i wykorzystaniu informacji dotyczących identyfikacji danej osoby. W kontekście pracy biurowej i administracyjnej w Państwowej Straży Pożarnej, może to oznaczać nieautoryzowane uzyskanie dostępu do kont i systemów informatycznych, a także do dokumentów i informacji poufnych. Ataki tego typu mogą prowadzić do poważnych szkód, takich jak utrata danych i poufności, a także do nieprawidłowej decyzji i działań podjętych w imieniu skradzionej tożsamości. Dlatego ważne jest, aby instytucje takie jak Państwowa Straż Pożarna stoso-

wały skuteczne środki zabezpieczenia, takie jak uwierzytelnianie dwuskładnikowe i szyfrowanie danych, aby zapobiec tego typu atakom.

Scenariusz kradzieży tożsamości w kontekście pracy biurowej w Państwowej Straży Pożarnej może wyglądać następująco:

1) Haker uzyskuje dostęp do poufnych informacji, takich jak nazwiska i adresy e-mail pracowników Państwowej Straży Pożarnej, dzięki włamaniu do systemu lub phishingowi.
2) Haker ukrywa swoją tożsamość i tworzy fałszywe konto e-mail podobne do rzeczywiste-go konta pracownika.
3) Haker wysyła e-maile do innych pracowników, w których żąda informacji lub załączników, takich jak hasła lub dokumenty finansowe. Pracownicy ufając pochodzeniu e-maila, ujawniają poufne informacje hakerowi.
4) Haker wykorzystuje uzyskane informacje do włamania do systemu i uzyskania dostępu do ważnych danych i informacji, takich jak dane osobowe czy finanse instytucji.

Taki atak może prowadzić do poważnych konsekwencji, takich jak utrata danych i poufnych informacji, co z kolei może wpłynąć na funkcjonowanie Państwowej Straży Pożarnej i jej wizerunek.

Aby przeciwdziałać atakom typu "Kradzież tożsamości" w kontekście pracy biurowej, administracyjnej w Państwowej Straży Pożarnej, należy zastosować następujące środki ostrożności:

1) Używanie silnych haseł i regularne ich zmienianie.
2) Wdrożenie dwuskładnikowego uwierzytelniania.
3) Zainstalowanie oprogramowania antywirusowego i regularne aktualizacje oprogramowania.
4) Ostrożne korzystanie z wiadomości e-mail i linków, które wydają się podejrzane.
5) Regularne tworzenie kopii zapasowych danych.
6) Wdrożenie polityki bezpieczeństwa danych i regularne szkolenia dla personelu.
7) Monitorowanie i raportowanie incydentów bezpieczeństwa.
8) Współpraca z zaufanymi dostawcami usług IT i cyberbezpieczeństwa.
10) Regularne testy penetracyjne, aby wcześniej wykryć potencjalne luki bezpieczeństwa.

Te środki ostrożności pozwolą na ochronę danych i systemów informatycznych Państwowej Straży Pożarnej przed atakami typu "Kradzież tożsamości".

- Złośliwy kod w poczcie elektronicznej

Atak typu "Złośliwy kod w poczcie elektronicznej" polega na wysłaniu złośliwego oprogramowania (złośliwego kodu) do użytkownika poprzez pocztę elektroniczną. Złośliwy kod może być ukryty w załączniku lub w treści wiadomości e-mail. Po otwarciu załącznika lub kliknięciu na link, złośliwe oprogramowanie może wykonać wiele działań, takich jak kradzież danych, zainfekowanie systemu, zablokowanie dostępu do danych itp. W kontekście pracy biurowej i administracyjnej w Państwowej Straży Pożarnej taki atak może mieć poważne konsekwencje, takie jak utrata danych, zakłócenie działania systemów, utrata produktywności i wprowadzenie chaosu w funkcjonowanie instytucji.

Przykładowy scenariusz tego typu ataku może wyglądać następująco:

1) Atakujący wysyła wiadomość e-mail z fałszywym nadawcą, który jest znanym i zaufanym pracownikiem Państwowej Straży Pożarnej.
2) Wiadomość zawiera załącznik lub link do pobrania, który jest ukrytym złośliwym oprogramowaniem.
3) Pracownik Państwowej Straży Pożarnej, który otrzymuje wiadomość, nieświadomie otwiera załącznik lub klika na link, co powoduje instalację złośliwego oprogramowania.
4) Złośliwe oprogramowanie uzyskuje dostęp do prywatnych danych pracownika i ich udostępnianie atakowi.
5) Atakujący może wykorzystać te dane do włamania się do systemów Państwowej Straży Pożarnej i uzyskania dostępu do wrażliwych informacji.

Aby przeciwdziałać atakowi typu "Złośliwy kod w poczcie elektronicznej" w Państwowej Straży Pożarnej, należy wdrożyć kilka środków bezpieczeństwa. Oto kilka przykładów:

1) Filtracja poczty: należy skonfigurować system filtrowania poczty elektronicznej tak, aby blokować załączniki i wiadomości zawierające złośliwy kod.
2) Ochrona antywirusowa: Wszystkie komputery powinny być zabezpieczone oprogramowaniem antywirusowym, które będzie w stanie wykryć i usunąć złośliwy kod.
3) Szkolenie pracowników: Pracownicy powinni być edukowani na temat niebezpieczeństw i zagrożeń związanych z pocztą elektroniczną, a także jak ich unikać.
4) Aktualizacje oprogramowania: Wszystkie oprogramowania, w tym oprogramowanie antywirusowe i system operacyjny, powinny być regularnie aktualizowane, aby zapewnić najlepsze zabezpieczenia.
5) Backup danych: Regularne tworzenie kopii zapasowych danych i plików jest kluczowe, aby umożliwić szybką i sprawną odbudowę danych w przypadku ataku.

- Atak na nienadzorowane urządzenie mobilne.

W dzisiejszych czasach urządzenia lokalne i mobilne są nieodłącznym elementem pracy w wielu instytucjach, w tym również w Państwowej Straży Pożarnej. Jednak brak monitoringu i zarządzania bezpieczeństwem tych urządzeń może stanowić poważne zagrożenie dla funkcjonowania instytucji i przechowywanych w niej danych. W razie włamania na urządzenie lub wirusa, dane i informacje na nim zgromadzone mogą zostać utracone lub nieuprawnione wykorzystane. Również brak możliwości kontrolowania i ochrony dostępu do danych na urządzeniach mobilnych może prowadzić do ich nieautoryzowanego przetwarzania lub ujawnienia. Dlatego ważne jest, aby Państwowa Straż Pożarna wdrożyła skuteczne rozwiązania do monitorowania i zarządzania bezpieczeństwem urządzeń, takie jak narzędzia szyfrujące dane i oprogramowanie antywirusowe, oraz regularne aktualizacje i szkolenia dla pracowników dotyczące bezpiecznego korzystania z urządzeń.

Przykładowy scenariusz może wyglądać następująco: W Państwowej Straży Pożarnej jest kilku pracowników, którzy używają swoich prywatnych laptopów, telefonów i tabletów do pracy z dostępem do ważnych informacji i danych. Jednak brak monitoringu i zarządzania bezpieczeństwem tych urządzeń oznacza, że nie są one zabezpieczone przed potencjalnymi zagrożeniami, takimi jak wirusy, złośliwe oprogramowanie czy hakerzy. W rezultacie jeden z pracowników może nieświadomie pobrać złośliwe oprogramowanie na swój prywatny laptop, które może uzyskać dostęp do ważnych danych i informacji, takich jak dane osobowe czy raporty dotyczące działalności Państwowej Straży Pożarnej. W takiej sytuacji dane te mogą zostać wykorzystane do niepożądanych celów lub ujawnione osobom trzecim, co może mieć poważne konsekwencje dla bezpieczeństwa i poufności informacji.

Aby przeciwdziałać atakom przez nienadzorowane urządzenie, należy zastosować kilka środków bezpieczeństwa, takich jak:

1) Zaawansowana kontrola dostępu: należy wdrożyć wymagane procedury uwierzytelniania i autoryzacji, aby zapewnić, że tylko upoważnione osoby mają dostęp do sieci i urządzeń.
2) Ochrona antywirusowa: należy zainstalować oprogramowanie antywirusowe na wszystkich urządzeniach i zapewnić jego regularne aktualizacje.
3) Monitoring i raportowanie: należy implementować rozwiązania monitorujące i raportujące, aby w czasie rzeczywistym śledzić działania na urządzeniach i wykrywać niepokojące zachowania.

4) Szkolenie i świadomość: należy zapewnić szkolenia dla pracowników dotyczące bezpieczeństwa urządzeń i zachęcać ich do świadomego i odpowiedzialnego korzystania z urządzeń mobilnych.
5) Aktualizacje i konserwacja: należy regularnie aktualizować oprogramowanie i sprzęt, aby zapewnić jego stabilność i bezpieczeństwo.

- Ataki internetowe i wewnętrzne – w tym zaawansowane ataki APT.

Ataki internetowe i wewnętrzne to działania zmierzające do uzyskania nieautoryzowanego dostępu do systemów i danych przechowywanych przez organizację, takie jak Państwowa Straż Pożarna. Złośliwe oprogramowanie i phishing są często wykorzystywane do inicjowania tego rodzaju ataków.

Zaawansowane ataki APT (Advanced Persistent Threats) to długoterminowe, zaawansowane ataki hakerskie skierowane na określoną organizację lub osobę. Celem jest kradzież lub zniszczenie informacji ważnych dla ofiary. Ataki APT często polegają na wykorzystywaniu słabych punktów bezpieczeństwa i luk w oprogramowaniu, aby uzyskać dostęp do systemów i danych ofiary.

Bez odpowiedniego monitorowania i zarządzania bezpieczeństwem, Państwowa Straż Pożarna może być narażona na poważne ataki internetowe i wewnętrzne, w tym na zaawansowane ataki APT, które mogą zagrozić poufności, integralności i dostępności danych i informacji ważnych dla działalności organizacji.

Ataki internetowe i wewnętrzne w tym APT (Advanced Persistent Threats) polegają na ciągłym i powolnym infiltrowaniu systemów i sieci celem zbierania wrażliwych informacji i danych.

Przykładowy scenariusz takiego ataku może wyglądać następująco:

1) Pozyskanie informacji o celu: Atakujący analizuje swoją ofiarę i uzyskuje dostęp do informacji publicznie dostępnych, takich jak adresy e-mail, nazwiska i numery telefonów pracowników, aby uzyskać dostęp do systemów i sieci wewnętrznych.
2) Infekcja poczty e-mail: Atakujący wysyła złośliwe wiadomości e-mail, które wyglądają na autentyczne i wydają się pochodzić z zaufanego źródła, do pracowników, zachęcając ich do kliknięcia w załącznik lub link.
3) Dostęp do sieci: Po kliknięciu w załącznik lub link, atakujący uzyskuje dostęp do sieci i systemów wewnętrznych, co pozwala im na zbieranie danych i kradzież informacji.
4) Monitorowanie i zbieranie informacji: Atakujący monitoruje systemy i sieci, zbierając wrażliwe informacje, takie jak hasła, numery kart kredytowych i inne poufne dane.

5) Wyprowadzanie danych: Atakujący wyprowadzają zebrane informacje z systemów i sieci, a następnie wykorzystują je do swoich celów.

W przypadku ataku APT, atakujący są w stanie utrzymać dostęp do systemów i sieci na długi czas, co oznacza, że atak może trwać miesiącami lub nawet latami, zanim zostanie wykryty.

Aby przeciwdziałać zaawansowanym atakom APT, należy:

1) Stosować zaawansowane technologie bezpieczeństwa: Włączenie technologii takich jak detekcja i blokowanie zaawansowanych zagrożeń oraz analiza bezpieczeństwa sieci.
2) Tworzenie kopii zapasowych danych: Utworzenie kopii zapasowej danych w kilku miejscach i regularne jej aktualizowanie pozwala na szybką i łatwą ochronę danych.
3) Monitorowanie ruchu sieciowego: Regularne monitorowanie ruchu sieciowego pozwala na wczesne wykrycie potencjalnych zagrożeń.
4) Edukacja pracowników: Przeszkolenie pracowników w zakresie bezpieczeństwa informatycznego i zdrowego rozsądku podczas korzystania z urządzeń służbowych.
5) Regularne aktualizacje oprogramowania: Regularne aktualizowanie oprogramowania zabezpieczeń oraz systemów operacyjnych zapewnia najlepszą ochronę przed nowymi zagrożeniami.
6) Współpraca z firmami bezpieczeństwa: Współpraca z profesjonalnymi firmami bezpieczeństwa pozwala na skuteczne reagowanie na zagrożenia i szybkie ich usuwanie.

• Zagrożenie „Nieuprawnione ujawnienie informacji – DLP”.

Zagrożenie "Nieuprawnione ujawnienie informacji" w obszarze DLP (Data Loss Prevention) polega na nieautoryzowanym przesyłaniu, kopiowaniu, drukowaniu lub ujawnianiu poufnych danych w organizacji. W kontekście pracy biurowej i administracyjnej w Państwowej Straży Pożarnej, takie zagrożenie może dotyczyć np. danych osobowych, informacji dotyczących bezpieczeństwa, dokumentów zawierających tajne informacje, itp. Nieodpowiedzialne lub nieodpowiednie wykorzystanie takich informacji może mieć poważne konsekwencje dla bezpieczeństwa i funkcjonowania organizacji.

Scenariuszem nieuprawnionego ujawnienia informacji może być na przykład sytuacja, w której pracownik Państwowej Straży Pożarnej wysyła e-mail z wrażliwymi informacjami dotyczącymi jednej ze spraw na nieodpowiedni adres e-mail. Albo sytuacja, gdy pracownik skanuje dokumenty zawierające wrażliwe informacje i przechowuje je na niezabezpieczonym urządzeniu, co pozwala na nieuprawnione ujawnienie tych informacji. W takich przypadkach nieodpowiednie zabezpieczenie danych i brak świadomości pra-

cowników dotyczące bezpieczeństwa informacji może prowadzić do poważnych konsekwencji dla Państwowej Straży Pożarnej i jej działalności.

Aby przeciwdziałać nieuprawnionemu ujawnieniu informacji w obszarze DLP, należy zastosować kilka środków bezpieczeństwa, w tym:

1) Klasyfikacja danych: Określenie wrażliwości danych i ich poziomu zabezpieczenia, co umożliwi wybór odpowiednich środków ochrony.
2) Kontrola dostępu: Ustanowienie ścisłych reguł dostępu do wrażliwych informacji i kontrola tego, kto je ujawnia.
3) Kryptografia: Szyfrowanie wrażliwych danych, aby uniemożliwić ich odczyt w przypadku wycieku.
4) Monitoring i detekcja incydentów: Stosowanie narzędzi do monitorowania i wykrywania nieuprawnionych ujawnień informacji.
5) Zabezpieczenie urządzeń i komunikacji: Wdrożenie zabezpieczeń fizycznych, takich jak blokady hasłami, i zabezpieczeń komunikacji, takich jak szyfrowanie połączeń sieciowych.
6) Szkolenie pracowników: Informowanie pracowników o zasadach bezpieczeństwa i wymaganiach w zakresie ochrony informacji oraz zapewnienie im odpowiedniej edukacji i szkoleń.
7) Plan incydentów: Opracowanie planu reagowania na incydenty związane z nieuprawnionym ujawnieniem informacji, aby szybko i skutecznie je zareagować.

- Zagrożenie Brak kontroli nad aplikacjami chmurowymi.

Brak kontroli nad aplikacjami chmurowymi oznacza, że istnieje ryzyko, że pracownicy Państwowej Straży Pożarnej będą używać nieautoryzowanych aplikacji lub narzędzi w chmurze, co może prowadzić do utraty danych, złamania bezpieczeństwa i innych zagrożeń związanych z cyberbezpieczeństwem. Duża liczba nad którymi administrator nie posiada kontroli dodatkowo utrudnia wykrywanie i kontrolowanie takich nieautoryzowanych aplikacji, co zwiększa ryzyko wystąpienia incydentów bezpieczeństwa. Aby zapobiec takim zagrożeniom, należy stosować rozwiązania do monitorowania i zarządzania aplikacjami chmurowymi, takie jak polityki bezpieczeństwa i kontrola dostępu, oraz edukować pracowników w zakresie bezpiecznego użytkowania aplikacji chmurowych.

Aby przeciwdziałać ryzyku braku kontroli nad aplikacjami chmurowymi w pracy biurowej i administracyjnej w Państwowej Straży Pożarnej, należy podjąć następujące kroki:

1) Zdefiniowanie i ujednolicenie polityki dotyczącej aplikacji chmurowych, w tym ich wykorzystywania, zarządzania i monitorowania.
2) Ograniczenie liczby aplikacji chmurowych, aby zapewnić, że administratorzy posiadają pełną kontrolę i widoczność.
3) Wdrożenie narzędzi do monitorowania i kontrolowania dostępu do aplikacji chmurowych, w tym zabezpieczenia i ochrony danych.
4) Regularne sprawdzanie aplikacji chmurowych pod kątem bezpieczeństwa i poprawianie ich, jeśli to konieczne.
5) Szkolenie pracowników w zakresie bezpiecznego korzystania z aplikacji chmurowych.
6) wykonywanie testów penetracyjnych i analizy bezpieczeństwa, aby zidentyfikować potencjalne luki i wyeliminować je.

- Brak monitoringu - ewidencji chronionych informacji.

Zagrożenie z brakiem monitoringu i ewidencji chronionych informacji może prowadzić do niekontrolowanego przepływu wrażliwych danych w środowisku biurowym Państwowej Straży Pożarnej. To z kolei może powodować poważne zagrożenie dla bezpieczeństwa i poufności informacji. Przykładowo, jeśli informacje są udostępniane i przechowywane bez odpowiedniej ewidencji i kontroli, istnieje ryzyko ich przypadkowego lub celowego wycieku.

W takim przypadku, rozwiązaniem jest stosowanie narzędzi dedykowanych pozwalających na automatyczne monitorowanie i wyszukiwanie informacji wrażliwych w środowisku chmurowym w którym przetwarza się dokumenty wytwarzane online w tym e-mail, co pozwala na zwiększenie kontroli nad nimi i zabezpieczenie przed nieautoryzowanym ujawnieniem. Narzędzia powinny umożliwiać również eksport danych do pliku, co pozwala na łatwiejsze prowadzenie dochodzeń i analiz.

Scenariusz może wyglądać następująco: w pracy biurowej i administracyjnej w Państwowej Straży Pożarnej, informacje są często przechowywane w chmurze, takiej jak O365. W związku z tym, jeśli nie ma żadnego monitorowania i ewidencji chronionych informacji, istnieje ryzyko, że nieautoryzowana osoba może uzyskać dostęp do tych informacji. Na przykład, może dojść do sytuacji, w której pracownik nieświadomie wysyła wrażliwe informacje na nieodpowiednie adresy e-mail. W takim przypadku, jeśli nie ma odpowiedniego monitorowania i ewidencji, może być trudno zidentyfikować, gdzie doszło do wycieku danych i jak szybko go naprawić.

Aby przeciwdziałać zagrożeniu braku monitoringu i ewidencji chronionych informacji w organizacji, należy przeprowadzić następujące działania:

7) Określenie zasad zarządzania informacją: Należy jasno określić, kto jest odpowiedzialny za zarządzanie informacją i jakie dane są uważane za poufne i wymagają specjalnej ochrony.
1) Monitorowanie dostępu do informacji: W celu ochrony informacji poufnych należy monitorować dostęp do nich i rejestrować wszelkie nieuprawnione działania.
2) Ochrona przed wyciekiem informacji: Należy zastosować odpowiednie środki bezpieczeństwa, takie jak szyfrowanie danych, ograniczenie dostępu do informacji czy stosowanie autentykacji dwuskładnikowej.
3) Regularne audyty bezpieczeństwa: Należy regularnie wykonywać audyty bezpieczeństwa, aby upewnić się, że wszystkie dane są odpowiednio chronione i że nie doszło do wycieku informacji.
4) Szkolenie pracowników: Pracownicy powinni być szkoleni w zakresie bezpieczeństwa informacji i jasno poinformowani o konsekwencjach nieprzestrzegania zasad bezpieczeństwa.
5) Stosowanie rozwiązań DLP: W celu zapewnienia odpowiedniego poziomu ochrony informacji należy stosować rozwiązania DLP (Data Loss Prevention), które pozwolą na automatyczne wykrywanie i blokowanie nieuprawnionego wycieku informacji.
6) Wykorzystanie narzędzi Advanced eDiscovery: W przypadku konieczności ujawnienia i odzyskania informacji warto wykorzystać narzędzie O365 Advanced eDiscovery, które pozwala na łatwe i szybkie odzyskanie informacji niezbędnych do przeprowadzenia audytu czy postępowania sądowego.

- Zagrożenia w obszarze braku korelacji zdarzeń z całej infrastruktury hybrydowej zarządzanej przez PSP.

Brak korelacji zdarzeń z całej infrastruktury jest poważnym zagrożeniem bezpieczeństwa w każdej organizacji, w tym w Państwowej Straży Pożarnej. W takim przypadku, jeśli kilka urządzeń i systemów generuje różne raporty bezpieczeństwa, administratorzy bezpieczeństwa nie mają jednolitego obrazu całej sytuacji. Może to prowadzić do niedostrzeżenia potencjalnego ataku lub incydentu, ponieważ każdy raport jest analizowany oddzielnie.

Należy posiadać narzędzia do zarządzania bezpieczeństwem, które umożliwia korelację zdarzeń z całej infrastruktury w jednym miejscu. Dzięki temu, administratorzy bezpieczeń-

stwa mają pełen obraz sytuacji, co pozwala na szybszą identyfikację i reakcję na incydenty.

Przykład: W Państwowej Straży Pożarnej zaobserwowano nieznane połączenia z siecią, ale raporty bezpieczeństwa z kilku urządzeń nie są ze sobą powiązane. Bez narzędzia do korelacji zdarzeń, administrator bezpieczeństwa może nie zauważyć, że te połączenia są częścią jednego ataku. W przypadku wykorzystania Azure Sentinel, połączenia te są łączone i analizowane jako część jednego incydentu, co pozwala na szybszą reakcję i zapobieganie dalszym szkodom.

Scenariusz zagrożenia braku korelacji zdarzeń z całej infrastruktury może wyglądać następująco:

Organizacja Państwowej Straży Pożarnej używa wielu różnych systemów i narzędzi, takich jak serwery, sieć, aplikacje, systemy bezpieczeństwa itp., ale nie jest w stanie połączyć danych i informacji z tych wszystkich źródeł. W rezultacie, gdy dojdzie do incydentu bezpieczeństwa, administratorzy nie są w stanie zidentyfikować źródła problemu, ponieważ dane są niekorelowane.

Na przykład, w jednym z systemów bezpieczeństwa pojawia się alarm, sygnalizujący podejrzaną aktywność, ale administratorzy nie są w stanie określić, skąd pochodzi problem, ponieważ nie mają dostępu do danych z innych systemów. W takiej sytuacji, organizacja jest narażona na poważne zagrożenie, ponieważ nie jest w stanie szybko reagować i chronić swoich danych i systemów.

W takim przypadku, wykorzystanie narzędzia do korelacji zdarzeń, takiego jak Azure Sentinel, może pomóc w integracji danych i informacji z różnych źródeł i umożliwiać administratorom szybsze i skuteczniejsze reagowanie na incydenty bezpieczeństwa.

Aby przeciwdziałać zagrożeniu braku korelacji zdarzeń z całej infrastruktury, należy zastosować narzędzia zintegrowane z systemami zabezpieczeń i wdrożyć strategię zarządzania zdarzeniami bezpieczeństwa (SIEM). W tym celu warto wykorzystać narzędzia SIEM które pozwala na śledzenie, analizę i korelację zdarzeń bezpieczeństwa z całej infrastruktury w czasie rzeczywistym. Warto również wdrożyć system automatycznego powiadamiania i reagowania na incydenty bezpieczeństwa, który pozwala na szybką reakcję w przypadku wystąpienia zagrożenia. Dodatkowo warto zapewnić ciągłe szkolenie personelu w zakresie bezpieczeństwa informacji oraz regularnie testować systemy bezpieczeństwa, aby upewnić się, że są one skuteczne i odpowiednio dostosowane do potrzeb organizacji.

SIEM (Security Information and Event Management) to system zarządzania informacjami i zdarzeniami dotyczącymi bezpieczeństwa. SIEM gromadzi dane dotyczące bezpieczeństwa z wielu różnych źródeł (np. firewall, system operacyjny, aplikacje, urządzenia sieciowe itp.), a następnie analizuje je i generuje raporty i alerty, które pomagają w identyfikacji i reagowaniu na potencjalne incydenty bezpieczeństwa. SIEM jest często wykorzystywany przez organizacje do monitorowania i zabezpieczania swoich systemów, w celu zapobiegania i reagowania na zagrożenia bezpieczeństwa, takie jak ataki hakerskie, nieautoryzowane dostępy, wycieki danych itp.

Podsumowując, zagrożenia związane z atakami na organizacje jest bardzo realne i powinno być brane poważnie. Atakujący wykorzystują coraz to nowsze i bardziej zaawansowane techniki, a łańcuch ataku (ang. Kill chain) i jego fazy gwarantują im pozyskanie cennych informacji. W celu zapobiegania takim incydentom, ważne jest, aby pracownicy organizacji zdawali sobie sprawę z zagrożeń związanych z bezpieczeństwem i wiedzieli jak się bronić przed atakami, na przykład poprzez regularne szkolenia i kampanie edukacyjne. Ponadto, należy zastosować odpowiednie narzędzia i technologie, takie jak systemy antywirusowe, filtry antyspamowe i narzędzia do wykrywania incydentów, które pomogą w wykrywaniu i zapobieganiu atakom. Wreszcie, organizacje powinny mieć plan reakcji na incydenty i regularnie testować jego skuteczność, aby mieć pewność, że są w stanie szybko i skutecznie reagować w przypadku zagrożenia.

W ramach oprogramowania dostępne są narzędzia, które są w stanie ograniczyć ryzyka związane z podatnościami bezpieczeństwa. Obecnie 96% ataków na organizacje rozpoczyna się poprzez wysłanie fałszywej wiadomości zawierającej link lub dokument z niebezpiecznym oprogramowaniem. Kampanie typu wykradanie poświadczenia pracownika i szyfrowanie stacji pracownika są obarczone bardzo dużym ryzykiem. Mitygacja tego ataku poprzez wykorzystanie technologii Defender for Office oraz drugi składnik uwierzytelnienia (MFA) pozwala minimalizować ten wektor ataku na organizacje.

Ataki na niezabezpieczone stacje pracowników lub urządzenia mobilne oraz uwierzytelnianie pracowników są także poważnymi zagrożeniami. Jeśli pracownik korzysta z zainfekowanej stacji, atakujący może uzyskać dostęp do informacji o hasłach i uwierzytelnianiu do systemów i wykradać wrażliwe dane bez kontroli przez dział bezpieczeństwa. Takie ataki są trudne do wykrycia. W celu zminimalizowania tych zagrożeń konieczne jest stosowanie narzędzi umożliwiających zarządzanie bezpieczeństwem stacji roboczych i/lub urządzeń mobilnych, na których wykonywane są powierzone zadania.

W przypadku zaawansowanych ataków na konta pracowników, możliwe jest wykrycie anomalii związanych z uwierzytelnianiem (np. logowanie poza godzinami pracy, logowanie do zasobów, do których pracownik nie miał dostępu) przy użyciu oprogramowania do zarządzania bezpieczeństwem.

Advanced Persistent Threat (APT) to nowoczesne metody ataków, w których wyspecjalizowane grupy starają się uzyskać dostęp do urzędu/organizacji i długotrwale monitorować jego systemy. Ataki te mogą wykorzystywać podatności "zero-day", a ich celem jest inwigilacja i atak na strukturę zarządzania siecią. Aby chronić się przed takimi atakami, ważne jest, aby monitorować nietypowe zachowania systemów i pracowników, a także mieć możliwość szybkiej reakcji na incydenty związane z bezpieczeństwem. Operacyjne centra bezpieczeństwa (SOC) powinny być w stanie wykryć i reagować na takie zagrożenia.

Wraz ze wzrostem znaczenia dostępu mobilnego i pracy zdalnej, rośnie waga ochrony tożsamości pracownika. Nazwa użytkownika i hasło do wielu systemów urzędu staje się wtedy kluczowym parametrem, który należy chronić. Kompromitacja tożsamości (przechwycenie tożsamości, kradzież haseł, podszywanie pod pracownika po przejęciu kontroli) powoduje utratę kontroli nad danymi i może skutkować wyciekiem danych z organizacji. Bardzo ważny jest również aspekt rozliczalności działań użytkowników (logowanie się do systemów) oraz dostęp do zasobów organizacji (emaile, dokumenty, bazy wiedzy). W celu przeciwdziałania kompromitacji tożsamości, należy korzystać z narzędzi i rozwiązań zapewniających monitorowanie i kontrolę działań użytkownika.

4.2.3 WDROŻENIE MECHANIZMÓW W ZAKRESIE URUCHAMIANIA AWARYJNYCH PLANÓW EWAKUACJI DYSPOZYTORÓW I DYŻURNYCH OPERACYJNYCH ORAZ SPRZĘTU TECHNICZNEGO W MIEJSCA ZASTĘPCZE.

Mając na uwadze cele strategii cyfryzacji PSP, niezbędnym staje się również określenie zunifikowanych sposobów postępowania w zakresie uruchamiania awaryjnych planów ewakuacji dyspozytorów i dyżurnych operacyjnych oraz sprzętu technicznego w miejsca zastępcze, pozwalających na bardziej optymalne przygotowanie do sytuacji awaryjnych i skuteczniejsze reagowanie w przypadku wystąpienia problemów związanych z funkcjonowaniem stanowiska kierowania, w tym wykorzystania jako węzły łączności

samochodów dowodzenia i łączności (SDł) lub nawet lekkich samochód rozpoznawczo ratowniczych (SLRr).

Na potrzeby zapewnienia funkcjonowania Stanowiska Kierowania Komendanta Głównego PSP zaplanowano zakup pojazdu specjalnie przystosowanego jako mobilny węzeł teleinformatyczny. Celem tego przedsięwzięcia jest zapewnienie ciągłości działania stanowiska oraz administracji, niezależnie od miejsca pracy i czasu. Mobilny węzeł teleinformatyczny będzie wyposażony w specjalistyczny sprzęt, taki jak zaawansowana sieć komputerowa, systemy telekomunikacyjne oraz oprogramowanie służące do zarządzania danymi i przepływem informacji. Dzięki temu pojazd będzie mógł pełnić rolę centrum dowodzenia i koordynacji działań w trakcie akcji ratowniczych czy w sytuacjach awaryjnych. W pojeździe tym, będzie również znajdowały się specjalistyczne systemy monitorujące pozwalające na śledzenie sytuacji na terenie akcji ratowniczej i na bieżące przekazywanie informacji do Komendanta Głównego PSP, jak i do pozostałych służb ratowniczych. Zakup ten pozwoli Państwowej Straży Pożarnej na zwiększenie skuteczności działań, a także na lepszą koordynację działań ratowniczych, niezależnie od miejsca ich prowadzenia. Mobilny węzeł teleinformatyczny jest niezbędnym narzędziem dla służb ratowniczych, które muszą być w stanie działać w każdych warunkach i w każdym miejscu.

Mając powyższe na uwadze, w szczególności zastosowania do opisanego podejścia pojazdów będących na wyposażeniu PSP, w tym także „Normę minimalnego wyposażenia bazy sprzętu specjalistycznego i środków gaśniczych" stanowiącą złącznik nr 6 do Rozporządzenia Ministra Spraw Wewnętrznych z dnia 21 listopada 2014 r. w sprawie szczegółowych zasad wyposażenia jednostek organizacyjnych państwowej straży pożarnej, w której określono, że:

- Lekki samochód rozpoznawczo-ratowniczy – stanowi wyposażenie każdej jednostce ratowniczo—gaśniczej (co najmniej jeden w powiecie musi być wyposażony w dwa radio-telefony oraz maszty zewnętrzne, a także radiporzeminnik)
- Samochód dowodzenia i łączności (kompanijne stanowisko dowodzenia) musi umożliwić dojazd w czasie do 60 minut w każde miejsce województwa,
- Samochód lub kontener dowodzenia i łączności (batalionowe stanowisko dowodzenia) musi być co najmniej jeden w województwie.

  W związku z powyższym należy:
  - opracować i wprowadzić dokument pn.: Standard wyposażenia samochodu specjalnego: Lekki samochód rozpoznawczo ratowniczy, typu SLRr.

- Standard wyposażenia samochodu specjalnego: Samochodu dowodzenia i łączności (batalionowe stanowisko kierowania), typu SDł bat.
- Standard wyposażenia samochodu specjalnego: Samochodu dowodzenia i łączności (kompanijne stanowisko kierowania), typu SDł komp.

Określenie zunifikowanych sposobów postępowania w zakresie uruchamiania awaryjnych planów ewakuacji dyżurnych operacyjnych i dyspozytorów oraz sprzętu technicznego w miejsca zastępcze, jest niezbędne w szczególności pod kątem wyposażenia i użycia Samochodów Dowodzenia i Łączności SDł (batalionowych i kompanijnych stanowisk kierowania - węzłów łączności) w przypadku wystąpienia sytuacji, w której niezależnie od przyczyn, stanowisko kierowania nie będzie w stanie realizować ustawowych zadań opisanych w Rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z dnia 17 września 2021 r. w sprawie szczegółowej organizacji krajowego systemu ratowniczo-gaśniczego opisanych w Rozdziale 9 pn. "Organizacja stanowisk kierowania".

Chcąc wdrożyć opisywane w niniejszym podrozdziale rozwiązania w PSP koniecznym jest również przeprowadzenie serii szkoleń, które pozwolą utworzyć w na poziome KG PSP pulę wykwalifikowanej kadry posiadającej kwalifikacje i umiejętności do samodzielnego efektywnego wykorzystania zespołu szeregu narzędzi.

Szkolenia dla użytkowników, pozwolą na pełne wykorzystanie nowych technologii i systemów, zwiększenie efektywności działań ratunkowych, poprawę bezpieczeństwa i ochrony danych, zwiększenie wydajności, poprawę jakości usług, ograniczenie problemów związanych z utrzymaniem, aktualizację wiedzy oraz poprawę komunikacji między różnymi jednostkami Państwowej Straży Pożarnej.

4.2.4 WDROŻENIE ZMIAN PRAWNO-FORMALNYCH.

Wdrażanie nowych usług teleinformatycznych oraz przeniesienie kluczowych usług do chmury obliczeniowej pozwalającej na lepsze wykorzystanie zasobów, usprawnienie procesów, zwiększenie bezpieczeństwa i redukcję kosztów, wymusza poza kwestiami szeroko rozumianego cyberbezpieczeństwa wdrożeniem stosownych zmian prawno-formalnych w zakresie wypracowania odpowiednich procedur, zasad, wytycznych, instrukcji, metodyk działań oraz porozumień z partnerami zewnętrznymi.

W związku z powyższym należy dokonać przeglądu dokumentacji, ze szczególnym uwzględnieniem współpracy w zakresie swoich kompetencji, w tym polegających na organizowaniu i prowadzeniu przedsięwzięć służących ochronie życia i zdrowia ludzi oraz

utrzymaniu bezpieczeństwa i porządku publicznego, przy jednoczesnym zachowaniu priorytetów własnych działań:

1. W ramach współpracy Państwowej Straż Pożarnej z Systemem Powiadamiania Ratunkowego – uzgodnienia z Krajowym Centrum Monitorowania Systemu Powiadamiania Ratunkowego MSWiA dot. aktualizacji:

- Szczegółowych procedur obsługi zgłoszeń alarmowych,
- Procedur przekazania zgłoszenia w sytuacji awaryjnej,
- Katalogu zdarzeń w Systemie Teleinformatycznym Centrów Powiadamiania Ratunkowego.

2. W ramach współpracy Państwowej Straż Pożarnej ze służbami, podmiotami i instytucjami prowadzącymi przedsięwzięcia służące ochronie życia i zdrowia ludzi oraz utrzymaniu bezpieczeństwa i porządku publicznego należy dokonać aktualizacji:

- Porozumienia z Komendantem Głównym Policji w sprawie współdziałania Państwowej Straż Pożarnej i Policji.
- Porozumienia z Dyrektorem LPR w sprawie współdziałania Lotniczego Pogotowia Ratunkowego z jednostkami ochrony przeciwpożarowej ksrg.
- Porozumienia z Dowódcą Wojsk Obrony Terytorialnej w sprawie współdziałania WOT i PSP.
- Porozumienia z Polskimi Sieciami Elektroenergetycznymi w sprawie współpracy Polskich Sieci Elektroenergetycznych i Państwowej Straży Pożarnej.
- Porozumienia z Komendantem Głównym Straży Granicznej o współdziałaniu i wzajemnej współpracy w zakresie zapobiegania i likwidowania zagrożeń.
- Porozumienia z Dowódcą Generalnym Rodzajów Sił Zbrojnych o współpracy pomiędzy Komendantem Głównym Państwowej Straży Pożarnej i Dowódcą Generalnym Rodzajów Sił Zbrojnych.
- Porozumienia z Dowódcą Operacyjnym Rodzajów Sił Zbrojnych o współpracy pomiędzy Komendantem Głównym Państwowej Straży Pożarnej i Dowódcą Operacyjnym Rodzajów Sił Zbrojnych.

Wyżej wymienione dokumenty określają warunki ścisłej współpracy, w tym kwestie pomocy na zasadach wzajemności, w zakresie:

- używania będących w dyspozycji Stron sił i środków (SiS) podczas działań ratowniczych;

- przygotowywania i aktualizowania analiz gotowości operacyjnej oraz planów ratowniczych stanowiących zbiór procedur postępowania podczas organizowania i prowadzenia działań ratowniczych;
- opracowania i uzgodnienia odpowiednich procedur dotyczących możliwości wykorzystania i dysponowania statków powietrznych na rzecz Państwowej Straży Pożarnej (PSP);
- realizacji działań ratowniczych wymagających wykorzystania specjalistów do spraw ratownictwa, specjalistycznego sprzętu oraz podstawowych i specjalistycznych technik ratowniczych;
- szkoleń, ćwiczeń i manewrów, w szczególności:
  - ćwiczeń i manewrów mających na celu weryfikację i doskonalenie procedur ratowniczych oraz podnoszenie poziomu wyszkolenia,
  - organizacji szkoleń strażaków jednostek ochrony przeciwpożarowej (JOP) włączonych do ksrg,
  - udostępnianiu śmigłowców do zajęć praktycznych oraz na potrzeby szkoleń członków specjalistycznych grup ratowniczych (SGR);
  - wymianę informacji i opinii na temat przydatności sprzętu i technik ratowniczych oraz współpracę przy wdrażaniu nowych rozwiązań technicznych oraz wymianę materiałów dydaktycznych i szkoleniowych;
  - wykorzystaniu: Krajowej Sieci Współdziałania ze Statkami Powietrznymi (KSWL) i Podpokładowej Sieci Współdziałania ze Statkami Powietrznymi (PSWL) na potrzeby współdziałania podczas prowadzenia działań ratowniczych, szkoleń, ćwiczeń i manewrów;
- bieżącej wymiany informacji pomiędzy stanowiskami kierowania PSP punktami kontaktowymi służb, podmiotów i instytucji:
  - wymiany doświadczeń w zakresie ratownictwa oraz w innych dziedzinach z zakresu ochrony ludności;
  - podejmowanie wspólnych działań promujących ratownictwo i ochronę ludności z wykorzystaniem statków powietrznych.

3. W ramach przeniesienia kluczowych usług do chmury obliczeniowej należy opracować szczegółowe wytyczne do sporządzania zasad organizacji dokumentacji stanowisk kierowania komendantów wojewódzkich Państwowej Straży Pożarnej i komendantów po-

wiatowych (miejskich) Państwowej Straży Pożarnej, uwzględniając przy tym następującą propozycje jednolitego podziału dokumentacji na:

Dokumentację podstawową w skład, której wejdzie:

- Dokumentacja organizacyjna w tym:
  - Regulaminy,
  - Wybrane akty prawne,
  - Zbiór zasad i wytycznych dot. funkcjonowania ksrg określonych przez KG PSP,
  - Plany, procedury i instrukcje postępowania.
- Dokumentacja operacyjna w tym:
  - Dokumentacja odwodów operacyjnych,
  - Zasoby ratownicze,
  - Mapy operacyjne z naniesionymi danymi dot. zabezpieczenia operacyjnego,
  - Działania ratownicze,
  - Wykaz teleadresowy PSP,
  - Współdziałanie krajowe,
  - Współdziałanie międzynarodowe,
  - Organizacja łączności.

Dokumentację pomocniczą w skład, której wejdzie:

- Harmonogramy służby w tym:
  - Harmonogramy czasu pełnienia służby 6-cio miesięczne,
  - Harmonogramy miesięczne,
  - Harmonogramy dyżurów miesięcznych KW i KP [M] PSP,
  - Harmonogramy dyżurów psychologów w PSP,
- Dokumentacja ewidencyjna w tym:
  - Książka przebiegu służby,
  - Książka poleceń służbowych,
  - Książka raportów grupy operacyjnej,
  - Książka ewidencji osób przebywających w SK, nieposiadających stosownych poświadczeń,
  - Książka pobierania kluczy do pomieszczeń służbowych,
  - Książka planowania służby,
  - Książka zamiany służby,
  - Meldunki o wypadkach ratowników podczas prowadzonych działań,

- Meldunki o wypadkach pojazdów PSP.

- Dokumentacja analityczna w tym:
  - Ewidencja zdarzeń,
  - Zestawienia dobowe zdarzeń,
  - Bieżąca analiza działań ratowniczo-gaśniczych (zdarzenia charaktery-styczne),
  - Raporty z pełnienia przebiegu służby,
  - Informacje dobowa SK PSP,
  - Raporty obsad SK PSP,
  - Monitoring racji żywnościowych,
  - Monitoring ćwiczeń,
  - Monitoring środka pianotwórczego,
  - Monitoring poziomu gotowości operacyjnej grup specjalistycznych ksrg,
  - Monitoring proszków gaśniczych,
  - Monitoring sytuacji meteorologicznej i hydrologicznej (IMGW),
  - Monitoring zabezpieczeń przejazdów SOP.

Dokumentację specjalną w skład, której wejdzie:

- Dokumentacja obronna jawna,
- Dokumentacja niejawna, w tym obronna niejawna.

Dokumentację uzupełniającą w skład, której wejdzie:

- Dokumentacja obrony cywilnej,
- Dokumentacja ochrony ludności,
- Dokumentacja zarządzania kryzysowego.

Poniżej przedstawione zostaną dokumenty programowo-strategiczne, w których ujęte są kwestie cyfrowe, obejmujące horyzont czasowy do 2030 roku, które mogą posłużyć do sfinansowania przedstawionej w tym rozdziale koncepcji zmian podczas wprowadzania przez Państwową Straż Pożarną strategii w zakresie transformacji cyfrowej - budowy i funkcjonowania systemów teleinformatycznych w Państwowej Straży Pożarnej:

1. Projekt strategia sprawne i nowoczesne państwo 2030,
2. Strategia Sprawne Państwo 2020,
3. Polityka dla rozwoju sztucznej inteligencji w Polsce do roku 2020
4. Droga ku cyfrowej dekadzie" do 2030 r.
5. Program zintegrowanej informatyzacji państwa,
6. Strategia cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019 – 2024;

WNIOSKI

Najogólniej rzecz ujmując bezpieczeństwo rozumiane jest jako moment, w którym nie ma zagrożenia . Nawiązując do bezpieczeństwa informacji, wiąże się to z nieprzerwanym działaniem procesów instytucji. Jest to stan, w którym informacje należące do instytucji nie są zagrożone, a do aspektów bezpieczeństwa informacji zaliczamy: dostępność, poufność, niezawodność, integralność, autentyczność.

Utrzymanie wysokiego poziomu bezpieczeństwa danych w sieciach komputerowych jest bardzo trudnym zadaniem. Budując systemy ochrony informatycy muszą uwzględnić wszystkie możliwe zagrożenia, biorąc także pod uwagę nielegalna działalność lokalnych pracowników organizacji.

W ramach systemu ochrony możemy wyszczególnić wiele rodzajów zabezpieczeń. Zalicza się do nich między innymi system zaporowy FIREWALL, programy antywirusowe lub karty uwierzytelniające tożsamość użytkowników. Z technicznej strony system zabezpieczeń danych w sieciach powinien zawierać wiele różnych, nawzajem się zabezpieczających i uzupełniających elementów.

Cyfryzacja jest niezbędna dla Państwowej Straży Pożarnej, aby stać się bardziej efektywną, skuteczną i nowoczesną instytucją. Wprowadzenie cyfryzacji to także szansa na zwiększenie zaufania obywateli do PSP i poprawę jakości świadczonych usług. Dlatego PSP powinno być liderem w procesie cyfryzacji i angażować się w działania zmierzające do jej wprowadzenia.

Państwowa Straż Pożarna musi być instytucją, która zdaje sobie sprawę z potrzeby cyfryzacji i modernizacji swojej działalności. W celu osiągnięcia tego celu, PSP powinno dążyć do stworzenie zespołów Citizen Developerów, które będą odpowiedzialne za tworzenie i rozwijanie aplikacji i narzędzi potrzebnych strażakom do wykonywania swoich obowiązków. Citizen Developerzy powinni współpracować z IT i powinni mieć dostęp do narzędzi typu Low-Code, No-code, które pozwolą im na szybkie i łatwe tworzenie oprogramowania dostosowanego do potrzeb strażaków.

Narzędzia typu Low-Code, No-code są coraz bardziej popularne w branży IT, ponieważ pozwalają one na szybkie tworzenie i implementację aplikacji bez potrzeby posiadania dużej wiedzy technicznej. Dzięki temu PSP będzie w stanie stworzyć oprogramowanie dostosowane do potrzeb strażaków, a także szybko reagować na zmiany i modyfikacje, które są konieczne w dynamicznie zmieniającym się świecie.

Głównym celem tworzenia Citizen Developerów i wykorzystania narzędzi typu Low-Code, No-code jest wyeliminowanie procesów obsługiwanych na papierze w ciągu najbliższych 5 lat.

Dzięki cyfryzacji i automatyzacji wielu procesów, PSP będzie w stanie znacznie usprawnić swoją działalność, a także udostępnić obywatelom dostęp do aktualnych i ważnych informacji, takich jak liczba pożarów i miejscowe zagrożenia, za pośrednictwem nowego portalu danych statystycznych.

Państwowa Straż Pożarna powinna także rozwijać i wspierać rolę Citizen Developerów w swojej organizacji. Wytypowani pracownicy, którzy posiadają odpowiednie umiejętności i zainteresowanie, będą mogli wspierać poza swoim podstawowym zakresem obowiązków PSP w tworzeniu aplikacji i narzędzi, które pomogą w realizacji ich misji poprzez wykorzystanie narzędzi typu Low-Code, No-code. Wówczas Państwowa Straż Pożarna będzie w stanie szybko i sprawnie tworzyć dedykowane oprogramowanie dla strażaków, które będzie dostosowane do ich potrzeb i wymagań.

Warto zaznaczyć, że celem Państwowej Straży Pożarnej powinna stać się nie tylko eliminacja procesów związanych z papierem, ale również usprawnienie i automatyzacja wielu procesów związanych z ich codzienną pracą. Dzięki temu strażacy będą mogli skoncentrować się na swoich głównych zadaniach i szybciej reagować na sytuacje zagrożenia.

Pozyskiwanie informacji i ich umiejętne wykorzystanie w trakcie podejmowania decyzji, warunkuje ich racjonalność i wpływa na efektywność procesu zarządzania strategicznego. Ponieważ część podejmowanych decyzji strategicznych powtarza się w pewnych cyklach (np. rocznych lub wieloletnich) uzasadnionym jest aby zasób informacji niezbędny do ich podejmowania nie był pozyskiwany w sposób jednorazowy (np. przez zatrudnienie ekspertów), a stanowił wewnętrznie spójny, stale odnawiany system, tworzony na własne potrzeby – tzw. systemem informacji strategicznej. Jego zadaniem jest pozyskiwanie, przetwarzanie, przechowywanie, ochrona i przekazywanie informacji dla potrzeb decyzji strategicznych, powtarzalnych.

Informacje będące podstawą decyzji niepowtarzalnych mogą być gromadzone w sposób incydentalny, bądź kupowane od zewnętrznych ekspertów. Z czasem część z nich zasila bazę danych systemu wzbogacając jego zasoby.

Użytkownicy systemu muszą być na bieżąco informowani o zasobach informacyjnych organizacji, aby mogli być przygotowani do roli aktywnego użytkownika informacji. To właśnie systemy informacyjne muszą wychodzić naprzeciwko oczekiwaniom użytkow-

ników, promować zasoby informacyjne tak, aby zachęcić zarówno kierowników jak i pracowników do aktywnego korzystania z dostępnych źródeł informacji, aby te wzajemne relacje system informacyjny-użytkownicy zaistniał w sposób właściwy niezbędna jest działalność szkoleniowa.

Działania związane ze szkoleniem użytkowników informacji powinny być dostosowane do różnego poziomu i rodzaju odbiorców ze znacznym naciskiem na naukę wyszukiwana informacji.

Istotne elementy umiejętnego korzystania z zasobów przez użytkowników obejmują:

- umiejętne rozpoznanie własnych potrzeb,
- wyszukiwanie odpowiedniej informacji spośród wielu innych,
- ocenę relewantności uzyskanych informacji oraz sposobu ich organizacji i przechowywania,
- efektywne i twórcze zastosowanie zgromadzonych danych.

Natomiast sama organizacja powinna zapewnić jak najlepszą, jak najszybszą obsługę systemu informacyjnego dla użytkowników poprzez udostępnianie:

- katalogów i własnych baz danych,
- katalogów i baz danych innych ośrodków poprzez sieci komputerowe
- informacji w rozległych sieciach komputerowych,
- baz za pośrednictwem sieciowego systemu baz danych.

W dzisiejszych czasach nie możliwe staje się funkcjonowanie jakiejkolwiek instytucji bez wykorzystania technologii informatycznych. Aby osiągać z nich korzyści należy przeprowadzać wnikliwie i stałe analizy procesów, technik itp. zespolonych z zastosowaniem wdrożeniowych przedsięwzięć informatycznych, które polegają na implementacji systemów informatycznych, które wspierają zarządzanie. Wprowadzania w życie tych przedsięwzięć informatycznych może odbywać się w przedstawionych poniżej etapach:

- Etap pierwszy jest to etap przygotowawczy. W tej części należy ustalić dokładne potrzeby funkcjonalne i technologiczne oraz cele, co do wdrażanego systemu informatycznego. Finalnymi efektami etapu pierwszego są wytypowane systemy informatyczne wspierające funkcjonowanie instytucji, które odpowiadają postawionym wcześniej wymaganiom.
- Etap drugi - wykonanie informatycznego planu wdrożeniowego według wytypowanej metodyki. Ten etap jest przeprowadzany w oparciu o umowę, która została zawarta

między dostawcą a nabywcą informatycznego planu wdrożeniowego. Ostatecznymi efektami drugiego etapu jest funkcjonujący system informatyczny wspierający funkcjonowanie organizacji.

- Etap trzeci - użytkowanie systemu informatycznego wspierającego funkcjonowanie instytucji, gdzie nabywcy na tym poziomie często podejmują decyzję o kooperacji z dostawcami w oparciu o umowę z gwarantowanym poziomem świadczenia usług - umowa serwisowa obsługi eksploatacyjnej wdrożonego systemu informatycznego wspomagającego zarządzanie, która zakłada utrzymanie i systematyczne poprawianie ustalonego między klientem a dostawcą poziomu jakości usług poprzez stały cykl zadań obejmujący: uzgodnienia, monitorowanie usługi, raportowanie, przegląd osiąganych wyników."

Podsumowując Państwowa Straż Pożarna powinna podjąć wyzwania cyfrowej transformacji i stać się liderem w tej dziedzinie. Poprzez tworzenie zespołów Citizen Developerów i wykorzystywanie narzędzi typu Low-Code, No-code, Państwowa Straż Pożarna jest w stanie szybko i skutecznie tworzyć oprogramowanie dostosowane do potrzeb strażaków i eliminować procesy obsługiwane na papierze. To wszystko przyczyni się do usprawnienia i automatyzacji w codziennej pracy, tej istotnie ważnej formacji dla bezpieczeństwa państwa, a także przyczyni się do zwiększenia bezpieczeństwa i ochrony obywateli.

ZAKOŃCZENIE

Niniejsza rozprawa doktorska stanowi efekt wielomiesięcznych dociekań autora w istotnie ważnej tematyce jaką jest bezpieczeństwo wewnętrzne państwa - a dokładniej wnikliwej analizy i oceny szeroko pojętego systemu informacyjnego oraz bezpieczeństwa systemu informacyjnego w organizacji zhierarchizowanej na przykładzie Państwowej Straży Pożarnej. Zrealizowane w ramach dysertacji badania umocniły autora w twierdzeniu o konieczności szerszego zainteresowania się niniejszą problematyką.

Celem pragmatycznym niniejszej pracy było opracowanie usprawnień w bezpieczeństwie systemu informacyjnego, poprawiających skuteczność funkcjonowania całej formacji Państwowej Straży Pożarnej, uwzględniając jej charakter jako organizacji zhierarchizowanej.

Rozwiązanie problemów szczegółowych oraz pozytywne zweryfikowanie hipotez szczegółowych umożliwiło rozwiązanie głównego problemu badawczego, które zostało zawarte w pytaniu: *Jakie zmiany wprowadzić w systemie bezpieczeństwa wymiany informacji w organizacji publicznej jaką jest Państwowa Straż Pożarna, tak aby poprawić skuteczność bezpieczeństwa obiegu informacyjnego?*

Dało to podstawę do potwierdzenia hipotezy głównej, która brzmiała: *Założono, że obecny system informacyjny w organizacji publicznej jaką jest Państwowa Straż Pożarna nie w pełni chroni informacje pozyskiwane i przetwarzane przez tą formację. Ułatwienie dostępu do danych, usprawnienie procesów przekazywania lub pobierania ich znacznych ilości w niewielkich jednostkach czasu oraz rozwój technologii przechowywania informacji mają ogromne znaczenie na funkcjonowanie tej instytucji. Natomiast odpowiednio przebiegający proces wymiany informacji wpływa między innymi na prawidłowe wykonywanie zadań, przy założeniu, że najważniejszymi aspektami bezpieczeństwa informacji są: dostępność, poufność, niezawodność, integralność i autentyczność.*

Przeprowadzone badania i uzyskane na ich podstawie wyniki, które zostały we wnikliwy i obszerny sposób przedstawione w rozdziale czwartym, potwierdzają, iż cel rozprawy został osiągnięty, a sformułowane problemy badawcze rozwiązane. Potwierdzona została również trafność przyjętych hipotez roboczych.

W pierwszej kolejności założono, że bardzo ważnymi elementami wpływającymi na skuteczność funkcjonowania instytucji Państwowej Straży Pożarnej jako organizacji zhierarchizowanej są ludzie z ich wiedzą, doświadczeniem i umiejętnościami, dopiero w dalszej kolejności struktura organizacyjna oraz system informacyjny, uwzględniając

przy tym zarówno otoczenie wewnętrzne jak i zewnętrze organizacji. Dokonano stwierdzenia, iż elementy te pełnią ważną rolę w kształtowaniu kultury tej organizacji. Diametralny wpływ na system informacyjny formacji Państwowej Straży Pożarnej jako organizacji zhierarchizowanej ma budowa jej struktury organizacyjnej, która przekłada się na zasięg i rozpiętość kierowania. To z kolei ma decydujący wpływ na szybkość przekazu danych i informacji oraz zniekształcenia w przepływie informacji w jednostce, zarówno pionie jak i poziomie struktury.
Dla poprawienia skuteczności funkcjonowania organizacji zhierarchizowanej konieczne jest wykorzystywanie adekwatnych do sytuacji form komunikowania się pomiędzy nadawcami, a odbiorcami informacji.

Niezmiernie istotnym faktem staje się również funkcjonowanie organizacji odpowiedzialnej za ważny obszar bezpieczeństwa państwa, jakim jest Państwowa Straż Pożarna w sytuacjach kryzysowych. Organizacja tego systemu ma bardzo realny wpływ na funkcjonowanie społeczności lokalnych zarówno podczas normalnego czasu jak i wstanie kryzysu, czy zagrożeń.

Bezpieczeństwo istniejącego systemu informacyjnego Państwowej Straży Pożarnej można usprawnić poprzez poprawę skuteczność obiegu informacji oraz zwiększenie efektywności zabezpieczeń. Aby tego dokonać należy ujednolicić systemy teleinformatyczne na wszystkich poziomach organizacyjnych tej formacji oraz wprowadzić zmiany pod kątem organizacyjnym, technicznym i funkcjonalnym w zasadach użytkowania, funkcjonowania i organizacji systemu informacyjnego. Istotne jest wdrożenie i utrzymanie właściwego systemu zarządzania bezpieczeństwem informacji, który będzie umożliwiał ochronę wszystkich przetwarzanych informacji, jak również zapewniał ciągłość realizowanych procesów i zadań. Aby osiągnąć jak najwyższy stopień bezpieczeństwa informacji, należy w odpowiedni sposób przygotować zasoby organizacji, a następnie odpowiednio i odpowiedzialnie nimi zarządzać. Niezbędne dla ochrony informacji w instytucji jest właściwie ułożenie i konsekwentne egzekwowanie polityki bezpieczeństwa informacji, co jest elementem decydującym o jej skuteczności, a systematyczny wielopłaszczyznowy nadzór zwiększa bezpieczeństwo informacji będących w obiegu.

Do głównych celów polityki bezpieczeństwa powinno należeć stworzenie reguł i zasad postępowania oraz wskazanie działań jakie należy podjąć, aby poprawnie zabezpieczyć dane. W ramach właściwego funkcjonowania polityki bezpieczeństwa nie należy umieszcza w niej zapisów które często podlegają zmianie, a także nie zawierać w treściach informacji szczegóło-

wej. W przeciwnym wypadku będzie występowała konieczność częstego przyjmowania nowych dokumentów. Polityka ta musi występować w formie pisemnej a każdy zatrudniony pracownik, który ma dostęp do przetwarzania danych osobowych obowiązkowo zapoznany z jej treścią.

Przeprowadzone badania pokazały, że system informacyjny w Państwowej Straży Pożarnej jest materią wielopłaszczyznowa i skomplikowaną. Przekaz informacji odbywa się zarówno w otoczeniu wewnętrznym jak zewnętrznym, a od poprawnie prowadzonej komunikacji zależy skuteczność i efektywność działań tej instytucji.

Dzięki zapewnieniu bezpieczeństwa systemu informacyjnego, polegającego na ograniczeniu, zminimalizowaniu lub wyeliminowaniu zagrożeń w przepływie informacji możliwe jest jej skuteczne i efektywne funkcjonowanie.

W ocenie autora dysertacji cel poznawczy, jakim była identyfikacja zagrożeń i możliwych usprawnień w systemie bezpieczeństwa informacji w Państwowej Straży Pożarnej jako organizacji publicznej został osiągnięty.

Przedstawione w niniejszej pracy wyniki badań mają uniwersalny, nowatorski charakter, pozwalający na ich dalszą modyfikację pod wpływem rozwoju dorobku naukowego.

Autor dysertacji wskazuje także możliwe i realne rozwiązania prowadzące do osiągnięcia w rzeczywistości celu pragmatycznego, co umożliwi jego zastosowanie w praktyce. Zaproponowane rozwiązania i wnioski nie zamykają jednak wachlarza ostatecznych możliwości i propozycji rozwiązań, które mogą zostać wykorzystane do doskonalenia systemu bezpieczeństwa informacyjnego, pozwalający na ich dalszą modyfikację pod wpływem rozwoju dorobku naukowego.

BIBLIOGRAFIA

Literatura:

1. Ackoff R. L., *Decyzje optymalne w badaniach stosowanych,* Wydawnictwo PWN, Warszawa 1969.
2. Adamski A., *Przestępczość w cyberprzestrzeni. Prawne środki przeciwdziałania zjawisku w Polsce na tle Konwencji Rady Europy*, Toruń 2001.
3. Ajdukiewicz K., *Język i poznanie, t. 2*. Wydawnictwo Naukowe. PWN, Warszawa 2006.
4. Aleksandrowicz T. R., *Komentarz do ustawy o dostępie do informacji publicznej*, Warszawa 2006.
5. Apanowicz J., *Metodologia nauk*, Wydawnictwo Dom Organizatora, Toruń 2003.
6. Apanowicz J., *Metodologia ogólna*, Wydawnictwo Wyższa Szkoła Administracji i Biznesu, Gdynia 2002.
7. Apanowicz J., *Metodologiczne elementy procesu poznania naukowego w teorii organizacji i zarządzania*, Wydawnictwo WSAiB, Gdynia 2000.
8. Apanowicz J., *Metodologiczne uwarunkowania pracy naukowej prace doktorskie prace habilitacyjne*, Wydawnictwo Difin, Warszawa 2005.
9. Armstrong M., Stephen T., *Zarządzanie zasobami ludzkimi*, Wydawnictwo Wolters Kluwer, Warszawa 2016.
10. Armstrong M., *Zarządzanie zasobami ludzkim*, Wydawnictwo Oficyna Ekonomiczna, Kraków 2004.
11. Bertalanffy von L., *Ogólna teoria systemów,* Wydawnictwo PWN, Warszawa 1984.
12. Bank J., *Zarządzanie przez jakość*, Wydawnictwo Felberg SJA, Warszawa 1999.
13. Bańka W., *Zarządzanie personelem*, Wydawnictwo Adam Marszałek, Toruń 2003.
14. Bańkowski A., *Słownik wyrazów obcych*, Wydawnictwo PWE, Warszawa 1997.
15. Bączek P., Zagrożenia informacyjne a bezpieczeństwo państwa polskiego, Adam Marszałek, Toruń 2006
16. Becała A., Pozyskiwanie, wykorzystanie i ochrona informacji w warunkach gospodarki opartej na wiedzy i społeczeństwa informacyjnego, Wydawnictwo Uniwersytetu Ekonomicznego we Wrocławiu, Wrocław 2018
17. Bennewicz M., *Coachnig złote zasady*, Wydawnictwo Helion, Gliwice 2018.
18. Bertalanffy von L., *Ogólna teoria systemów,* Wydawnictwo PWN, Warszawa 1984.
19. Białową P., *Benchmarking i Business Process Reengineering- wzajemne zależności*, „Problemy Jakości" 2000, nr 11, Warszawa 2000.
20. Bild J., Gornall S., *Sztuka coachingu. Zbiór narzędzi i wskazówek*, Wydawnictwo Galaktyka, Łódź 2017.
21. Bogan C. E., English M.J., *Benchmarking jako klucz do najlepszych praktyk*, Wydawnictwo Helion, Gliwice 2006.
22. Bogdanienko J., Wiedza i innowacje w firmie, AON, Warszawa 2011.
23. Bordowski J., Dyrda M. i in., Człowiek w organizacji, Elipsa, Warszawa 2001.
24. Borowiecki R., Czekaj J. (red.), Zarządzanie zasobami informacyjnymi w warukach nowej gospodarki, Difin SA, Warszawa 2010
25. Bojańczyk M., *Regresja i korelacja na światowych rynkach- w pułapce metod ilościowych*, „Kwartalnik Naukowy Uczelni Vistula", nr 4, 2013.
26. Bramley P., *Ocena efektywności szkoleń*, Wydawnictwo Dom Wydawniczy ABC, Kraków 2001.
27. Brilman J., *Nowoczesne koncepcje i metody zarządzania*, Wydawnictwo PWE, Warszawa 2002.

28. Bugdol M., *Zarządzanie jakością w urzędach administracji publicznej*, Zeszyty Naukowe Uniwersytetu Przyrodniczo-Humanistycznego w Siedlcach, Warszawa 2008.
29. Castells M., *Społeczeństwo sieci*, Wydawnictwo Naukowe PWN, Warszawa 2007.
30. Ciborowski L., *Walka informacyjna*, Europejskie Centrum Edukacyjne, Toruń 1999.
31. Ciborowski L., Walka informacyjna, Adam Marszałek, Toruń 2001
32. Cienińska B., Łunarski J., Perłowski R., Stadnicka D., Systemy zarządzania bezpieczeństwem w przedsiębiorstwie, Oficyna Wydawnicza Politechniki Rzeszowskiej, Rzeszów 2006
33. Cieślarczyk M. (red. nauk), *Metody, techniki i narzędzia badawcze oraz elementy statystyki,* Wydawnictwo AON, Warszawa 2003.
34. Cieślarczyk M. (red. nauk.), *Metody, techniki i narzędzia badawcze oraz elementy statystyki stosowane w pracach magisterskich i doktorskich*, Wydawnictwo AON, Warszawa 2006.
35. Clarke A., *e-learning nauka na odległość*, Wydawnictwo Komunikacji i Łączności WKŁ, Warszawa 2016.
36. Clutterbuck D., *Każdy potrzebuje mentora*, Wydawnictwo PETIT, Warszawa 2002.
37. Czakon W, *Podstawy metodologii w naukach o zarządzaniu*, Wydawnictwo Oficyna, Warszawa 2013.
38. Czarkowska L.D., *Bussiness coaching jako dźwignia rozwoju przedsiębiorczości*, Wydawnictwo Poltext, Warszawa 2015.
39. Czarkowska L.D., *Coaching jako klucz do wewnętrznej motywacji,* Wydawnictwo Poltext, Warszawa 2017.
40. Czarkowska L.D., *Coaching jako konstruktywny dialog,* Wydawnictwo Poltext, Warszawa 2016.
41. Czupryński A., Wiśniewski B., Zboina J., *Nauki o bezpieczeństwie – Wybrane problemy badań*, Wydawnictwo CNBOP-BIP, Józefów 2017.
42. Dobrowolski Z., *Szkolenie pracowników*, Wydawnictwo Organon, Zielona Góra 2002.
43. Drozd A., Ustawa o ochronie danych osobowych. Komentarz. Wzory pism i przepisy, Lexis Nexis, Warszawa 2007.
44. Drucker P. F., Praktyka zarządzania, MT Biznes, Kraków 1994.
45. Dziuba D. T., Gospodarki nasycone informacją i wiedzą, Uniwersytet Warszawski, Warszawa 2000.
46. Ehrlich A., *Innowacja i przedsiębiorczość: praktyka z zasady*, Państwowe Wydawnictwo Ekonomiczne, Warszawa 1992.
47. Filek J., *Wprowadzenie do etyki biznesu*, Wydawnictwo AE w Krakowie, Kraków 2004.
48. Fischer B., *Przestępstwa komputerowe i ochrona informacji*, Kraków 2000.
49. Fiszer K., Markiewicz D., *Ochrona przed pożarami i innymi nadzwyczajnymi zagrożeniami*, tom I Wydawnictwo ZPP Warszawa 2008.
50. Flakiewicz W., *Podejmowanie decyzji kierowniczych,* Wydawnictwo PWE, Warszawa.
51. Flakiewicz W., Systemy informacyjne w zarządzaniu. Uwarunkowania, technologie, rodzaje, C. H. Beck, Warszawa 2012
52. Forlicz S., Informacje w biznesie, PWE, Warszawa 2008.
53. Gałązka M., *Zasady prowadzenia walki informacyjnej*, Bellona nr 1, 2007.
54. Gleń A., *Podstawy poznawcze badań bezpieczeństwa narodowego*, Zeszyty Naukowe AON 2(83) 2011.

55. Gierszewska G., Romanowska M., Analiza strategiczna przedsiębiorstwa, PWN, Warszawa 1997.
56. Glinkowska B., *Modelowanie w procesach usprawniania organizacji – uwagi teoretyczno-metodyczne*, „Acta Universitatis Lodziensis. Folia Oeconomica", Zeszyt 234, 2010.
57. Gościński J., *Projektowanie systemów zarządzania*, Wydawnictwo PWN, Warszawa 1971.
58. Griffin R. W., *Podstawy zarządzania organizacjami*, Wydawnictwo PWN, Warszawa 1997.
59. Griffin R., *Podstawy zarządzania organizacjami*, Wydawnictwo Naukowe PWN, Warszawa 2020.
60. Grodzki R., *Zarządzania kryzysowe. Dobre praktyki,* Wydawnictwo Difin, Warszawa 2020.
61. Grudzewski W. M., Jagusztyn-Grochowska S., Zużewicz L., *Benchmarking- istota i zastosowanie* „Ekonomika i organizacja przedsiębiorstw", 1999, nr 7.
62. Guzewski P., Wróblewski D., Małozięć D*, Czerwona Księga Pożarów - Tom I.*, Wydawnictwo CNBOP, Józefów 2016.
63. Guzewski P., Wróblewski D., Małozięć D*, Czerwona Księga Pożarów - Tom II.*, Wydawnictwo CNBOP, Józefów 2016.
64. Haman W., Gut J., *Coaching narzędziowy*, Wydawnictwo Helion, Gliwice 2015.
65. Hetmański M., Świat informacji, Difin, Warszawa 2015.
66. Hopej M., Kral Z., *Współczesne metody zarządzania w teorii i praktyce,* Wydawnictwo Oficyna Wydawnicza Politechniki Wrocławskie, Wrocław 2011.
67. Idrian P., *Doskonalenie kompetencji społecznych wojskowych nauczycieli akademickich*, Wydawnictwo Akademia Sztuki Wojennej, Warszawa 2018.
68. Jabłoński M., *Kompetencje pracownicze w organizacji uczącej się. Metody doskonalenia i rozwoju*, Wydawnictwo C.H. Beck, Warszawa 2009.
69. Jakubczak R., Marczak J., *Bezpieczeństwo narodowe Polski w XXI wieku. Wyzwania i strategie*, Wydawnictwo Bellona, Warszawa 2011.
70. James W., *Pragmatyzm*, Wydawnictwo Zielona Sowa, Kraków 2005.
71. Jemielniak D., Koźmiński A. K. (red.), Zarządzanie wiedzą, WAiP, Warszawa 2008.
72. Janasz W., Kozioł K., D*eterminanty działalności innowacyjnej przedsiębiorstw*, Polskie Wydawnictwo Ekonomiczne, 2007.
73. Januszek H., *Gospodarowanie zasobami Państwowej Straży Pożarnej w Wielkopolsce*, Wydawca Komenda Wojewódzka PSP w Poznaniu, Poznań 2014.
74. Kaczmarek A., *Obowiązki administratorów danych osobowych przetwarzających dane osobowe w systemach informatycznych rejestrujących usługi medyczne*, [w:] *Ochrona danych medycznych i ich przetwarzanie. Materiały konferencji naukowo-szkoleniowej*, Warszawa 2000.
75. Kaczmarek T., *Metodologia badań naukowych o wiedzy i prawdzie w naukach ekonomicznych*, Wydawnictwo Oficyna Wydawnicza Uczelni Łazarskiego, Warszawa 2010.
76. Kalinowski M., *Dylematy projektowania i stosowania symulacyjnych gier decyzyjnych w rozwoju pracowników,* nr 14, Zarządzanie i Finanse Journal of Management and Finance, 2016.
77. Kamińska L, *Zasady dostępu do informacji publicznej oraz stosunek ustawy o dostępie do informacji publicznej do innych ustaw*, KPP 2012, z. 3.
78. Karwala S., *Mentoring jako strategia wspierająca wszechstronny rozwój osobisty*, Wydawnictwo Wyższa Szkoła Biznesu- National Louis University, Nowy Sącz 2019.

79. Kauf S., Tłuczak A., *Metody i techniki badań ankietowych na przykładzie zachowań komunikacyjnych opolan*, Wydawnictwo Uniwersytet Opolski, Opole 2013.
80. Kitler W., *Obrona narodowa III RP. Pojęcie. Organizacja. System*, „Zeszyty Naukowe AON" (dodatek), Warszawa 2002.
81. Kitler W., *Bezpieczeństwo narodowe RP. Podstawowe kategorie. Uwarunkowania. System*, Wydawnictwo AON, Warszawa 2011.
82. Kisperska- Moroń D., *Benchmarking jako narzędzie zarządzania logistycznego*, Wydawnictwo Akademia Ekonomiczna w Katowicach, Katowice 2002.
83. Kolegowicz K., Informacja w zarządzaniu przedsiębiorstwem, red. Borowiecki R., Kwieciński M., Zakamycze, Kraków 2003.
84. Konarski X., *Nowe zasady i tryb udostępniania danych osobowych*, [w:] *Nowelizacja ustawy o ochronie danych osobowych 2010*, red. G. Sibiga, dodatek do MoP2011, nr 3.
85. Koralewicz J., Ziółkowski M., *Sposoby myślenia o gospodarce.* Warszawa: PWE, 2000.
86. Kręcikij J., *Istota działań sieciocentrycznych*, Zeszyty Naukowe Akademii Obrony Narodowej, nr 4, 2006.
87. Klepacki B., *Wybrane zagadnienia związane z metodologią badań naukowych*, Wydawnictwo Roczniki Nauk Rolniczych, Warszawa 2009.
88. Kompała A., *Istota Zagrożeń*, Obronność Wydawnictwo AON. Zeszyty Naukowe 3(11)/2014.
89. Korzeniowski R., *Wstęp do metodologii badań bezpieczeństwa narodowego*, Wydawnictwo Instytut Nauk Politycznych Uniwersytetu Warmińsko- Mazurskiego w Olsztynie, Olsztyn 2013.
90. Kossakowska M., Sołtysińska I., *Szkolenie pracowników a rozwój organizacji*, Wydawnictwo Oficyna Ekonomiczna, Kraków 2002.
91. Kostera M., *Zarządzanie personelem*, Polskie Wydawnictwo Ekonomiczne, Warszawa 1999.
92. Kotarbiński T., *O pojęciu metody*, Wydawnictwo PWN, Warszawa 1957.
93. Kotarbiński T., *Traktat o dobrej robocie,* Wydawnictwo Zakład im. Ossolińskich, Wrocław 1955.
94. Kotarbiński T., *O pojęciu metody*, Wydawnictwo PWN, Warszawa 1957.
95. Koźmiński A. K., *Analiza systemowa organizacji*, Wydawnictwo PWE, Warszawa 1976.
96. Kożuch A., Kożuch B., Sułkowski Ł., Bogacz-Wojtanowska E.. Lewandowski M., Krzemińska A., *Państwowa Straż Pożarna w Działaniach Poza Granicami Kraju*, Obronność, Zeszyty Naukowe 3(19)/2016.
97. Król H. Ludwiczyński A.*, Zarządzanie zasobami ludzkimi. Tworzenie kapitału ludzkiego organizacji*. –Warszawa: PWN. 2007.
98. Krzykała F., *Metodologia badań i technik badawczych socjologii gospodarczej*, Wydawnictwo Akademii Ekonomicznej, Poznań 2001.
99. Kulawiecka E., *Rachunek korelacji w naukach o bezpieczeństwie z wykorzystaniem programu Statistica*, Wydawnictwo Obronność - Zeszyty Naukowe Wydziału Zarządzania i Dowodzenia Akademii Obrony Narodowej, Numer 4(20) (2016 r.), s. 370.
100. Kuc B. R., *Funkcje nauki. Wstęp do metodologii. Nauka nie jest grą*, Wydawnictwo Menedżerskie PTM, Warszawa 2012.
101. Kurzępa B., Ustawa z dnia 24 sierpnia 1991 r. o ochronie przeciwpożarowej. Komentarz, Wydawnictwo „Dom Organizatora", Toruń 2013.
102. Kuźmicz K.A., *Benchmarking procesowy jako instrument doskonalenia zarządzania uczelnią*, Wydawnictwo Wolters Kluwer SA., Warszawa 2015.

103. Kwieciński M., *Bezpieczeństwo – wymiar współczesny i perspektywy badań*, Oficyna Wydawnicza AFM, Kraków 2010.
104. Lacek G., *Ratownictwo powszechne – koncepcja funkcjonowania*, „Zeszyt Problemowy Towarzystwa Wiedzy Obronnej" 1996.
105. Lambert T., *Problemy zarządzania. 50 praktycznych modeli rozwiązań,* Wydawnictwo Dom Wydawniczy ABC, Warszawa 1999.
106. Liedel K., Piasecka P., Aleksandrowicz T.R., Analiza informacji. Teoria i praktyka, Difin, Warszawa 2012.
107. Liedel K., Bezpieczeństwo informacyjne w dobie terrorystycznych i innych zagrożeń bezpieczeństwa narodowego, Adam Marszałek, Toruń 2008.
108. Liedel K., Serafin T., Otwarte źródła informacji w działalności wywiadowczej, Difin, Warszawa 2011.
109. Lisiecki M., *Zarządzanie bezpieczeństwem publicznym*, Wydawnictwo ŁÓŚGRAF, Warszawa 2011.
110. Łagan J., Gontarz K**.,** *Jak efektywnie szkolić pracowników*?- Warszawa: Polska Agencja Rozwoju Przedsiębiorczości, 2009.
111. Łoś-Nowak T., Bezpieczeństwo, [w:] Leksykon politologii, red. A. Antoszewski, R. Herbut, Alta 2, Wrocław 2003.
112. Łuczak J. (red.), Zarządzanie bezpieczeństwem informacji, Oficyna Współczesna, Poznań 2004.
113. Łucewicz J., *Zarządzanie zasobami ludzkimi. Zagadnienia wybrane*, Wydawnictwo Naukowe PWN, Warszawa 1995.
114. Maciejewski M., Prawo informacji – zagadnienia podstawowe, [w:] Prawo informacji. Prawo do informacji, red. W. Góralczyk, WSPiZ im. L. Koźmińskiego, Warszawa 2006.
115. Madej M., Rewolucja informatyczna – istota, przejawy oraz wpływ na postrzeganie bezpieczeństwa państw i systemu międzynarodowego, [w:] Bezpieczeństwo teleinformatyczne państwa, red. M. Madej, M. Terlikowski, PISM, Warszawa 2009.
116. Machaczka J., *Zarządzanie rozwojem organizacji. Czynniki, modele, strategia, diagnoza,* Wydawnictwo PWN, Warszawa-Kraków 1998.
117. Maddux R.B., *Budowanie zespołu Wydanie II,* Wydawnictwo Helion, Gliwice 2006.
118. Madej M., *Zagrożenia asymetryczne*, PISM, Warszawa 2007.
119. *Majchrzak M., Effective Public Management in Local Government. EUROPEAN JOURNAL OF SCIENCE AND RESEARCH 1/2017, s. 49-56.*
120. Majewski T., *Ankieta i wywiad w badaniach naukowych*, Wydawnictwo AON, Warszawa 2002.
121. Makowiec P., *Poradnik metodyczny instruktora*, Wydawnictwo Dowództwa Wojsk Obrony Terytorialnej - Legii Akademickiej Ministerstwa Obrony Narodowej, Warszawa 2018.
122. Marek S., *Elementy nauki o przedsiębiorstwie*, Wydawnictwo Economicus, Szczecin 2001.
123. Maslow A., *Teoria ludzkich potrzeb* w: „Przegląd psychologiczny", Toronto 1943.
124. Masłyk Musiał E., *Ludzie w świecie biznesu*, Oficyna Wydawnicza WSM SIG, Warszawa 2000.
125. Mayo A., *Kształtowanie strategii szkoleń i rozwoju pracowników*, Wydawnictwo Oficyna Ekonomiczna, Kraków 2002.
126. McKenna E., Beech N., *Zarządzanie zasobami ludzkimi*, Wydawnictwo Felberg SJA, Warszawa 1999.
127. Michniak J. i in., *Organizacja dowodzenia jednostkami operacyjnymi wojsk lądowych*, cz. 3. Proces dowodzenia, AON, Warszawa 1998.

128. Milczarek E., *Ograniczenia praw i wolności obywatelskich w obliczu zagrożenia terrorystycznego*, [w:] *Oblicza współczesnego terroryzmu,* pod red. G. Libora, Wydawnictwo internetowe e-bookowo, Szczecin 2016.
129. Nachmias D., *Metody badawcze w naukach społecznych*, Wydawnictwo Zysk i S-ka, Poznań 2001.
130. Niewiadomski Z., *Samorząd terytorialny. Ustrój i gospodarka*, Oficyna Wydawnicza Branta, Warszawa 2001.
131. Nowacki T., *Teoretyczne podstawy opracowań metodycznych*, Wydawnictwo Polskiej Akademii Nauk, Wrocław 1976.
132. Nowak E.,Głowiński K., *Teoretyczne metody badawcze w naukach społecznych,* Wydawnictwo Obronność - Zeszyty Naukowe Wydziału Zarządzania i Dowodzenia Akademii Obrony Narodowej nr 2.
133. Nowak S., *Metodologia badań społecznych*, Wydawnictwo PWN, Warszawa 1985.
134. Nowak W., Nowak E., *Podstawy logistyki w sytuacjach kryzysowych z elementami zarządzania logistycznego*, Wydawnictw Społeczna Wyższa Szkoła Przedsiębiorczości i Zarządzania, Łódź 2009.
135. Nowak E., *Zarządzanie kryzysowe w sytuacjach zagrożeń niemilitarnych*, Wydawnictwo AON, Warszawa 2007.
136. Nowak A., Scheffs W., Zarządzanie bezpieczeństwem informacyjnym, AON, Warszawa 2010.
137. Nowak E., Nowak M., Zarys teorii bezpieczeństwa narodowego, Difin SA, Warszawa 2011.
138. Nowosielski S. (red.), *Podejście procesowe w organizacjach*, Prace naukowe Uniwersytetu Ekonomicznego we Wrocławiu, nr 169, 2011.
139. Nowak S., *Metodologia badań społecznych*, Wydawnictwo PWN, Warszawa 1985.
140. O'Neill M.B., *Coaching dla kariery menadżerskiej*, Wydawnictwo REBIS, Poznań 2005.
141. Okoń W., *Słownik pedagogiczny,* Wydawnictwo PWN, Warszawa 1975.
142. Okoń W., *Wprowadzenie do dydaktyki ogólnej*, Wydawnictwo Akademickie Żak, Warszawa 1998.
143. Oleksyn T., *Sztuka kierowania*, Wydawnictwo Wyższa Szkoła Zarządzania i Przedsiębiorczości im. B. Jańskiego, Warszawa 2001.
144. Olszewski R., *Bezpieczeństwo współczesnego świata*, wyd. Adam Marszałek, Toruń 2006.
145. Parsloe E., Wray M, *Trener i mentor – udział coachingu i mentoringu w doskonaleniu procesu uczenia się*, Wydawnictwo Oficyna Ekonomiczna, Kraków 2002.
146. Pelc M., *Elementy metodologii badań naukowych*, Wydawnictwo AON, Warszawa 2009.
147. Penc-Pietrzak I., *Równaj do najlepszych „Manager",* 2000, nr 2.
148. Penkowska G., *Meandry e-learningu,* Wydawnictwo PWN, Warszawa 2008.
149. Pieter J., *Ogólna metodologia pracy naukowej,* Wydawnictwo Zakładu Narodowego im. Ossolińskich, Wrocław 1967.
150. Pietrasiński Z., *Sztuka uczenia się*, Wydawnictwo Wiedza Powszechna, Warszawa 1975.
151. Pietrasiński Z. *Rozwój człowieka dorosłego.*-Warszawa: PWN, 1990.
152. Pilch T., Bauman T., *Zasady badań pedagogicznych. Strategie ilościowe i jakościowe,* Wydawnictwo Akademickie „Żak", Warszawa 2001.
153. Pipkin D.L., Bezpieczeństwo informacji, Wydawnictwa Naukowo-Techniczne, Warszawa 2002 75. Piwowarski J., Transdyscyplinarna istota kultury bezpieczeństwa narodowego, Wydawnictwo Naukowe Akademii Pomorskiej, Słupsk 2016.

154. Piwowarski L. W., *Poradnik przygotowania i prowadzenia ćwiczeń w zakresie zarządzania kryzysowego i obrony cywilnej*, Mazowiecki Urząd Wojewódzki, Warszawa 2007.
155. Pocztowski A., *Zarządzenie zasobami ludzkimi*, Wydawnictwo Polskiego Towarzystwa Ekonomicznego, Warszawa 2003.
156. Polak B., *Podstawy teorii kształcenia*, Wydawnictwo Szczecińska Szkoła Wyższa Collegium Balticum, Szczecin 2013.
157. Pomykało W., *Encyklopedia pedagogiczna*, Wydawnictwo Fundacja Innowacja, Warszawa 1993.
158. Polski Komitet Normalizacyjny. „Technika informatyczna. Praktyczne zasady zarządzania bezpieczeństwem informacji". PN-ISO/IEC 17799, Warszawa 2003.
159. Potejko P., Bezpieczeństwo informacyjne, [w:] Bezpieczeństwo państwa, red. K. A. Wojtaszczyk, A. Materska-Sosnowska, ASPRA-JR, Warszawa 2009
160. Praca zbiorowa, *Metodologia badań politologicznych*, Wydawnictwo Polskie Towarzystwo Nauk Politycznych, Warszawa 2016.
161. Praca zbiorowa*, Innowacyjne Technologie w Straży Pożarnej,* Wydawnictwo CNBOP-BIP, Józefów 2018.
162. Praca zbiorowa – *Ochrona przeciwpożarowa a bezpieczeństwo państwa*, Wydawnictwo CNBOP-PIB, Józefów 2014.
163. Pszczołowski T., *Mała encyklopedia prakseologii i teorii organizacji*, Wydawnictwo Zakład Narodowy im. Ossolińskich, Wrocław-Warszawa-Kraków-Gdańsk 1978.
164. R. D. Petrin, *Najlepsze praktyki w profesjonalnym mentoringu, prezentacja z kongresu* Kadry 2010.
165. Rogers J., Coaching. *Podstawy umiejętności*, Wydawnictwo Gdańskie Wydawnictwo Psychologiczne, Gdańsk 2013.
166. Roguski J., Innowacyjne technologie w Straży Pożarnej, Wydawnictwo CNBOP-BIP, Józefów 2018.
167. Rybak M.(red.), *Kapitał ludzki a konkurencyjność przedsiębiorstw*. - Warszawa: Poltext, 2003.
168. Rybak M., *Szkolenie i doskonalenie pracowników*, Oficyna Wydawnicza Szkoły Głównej Handlowej, Warszawa 1998.
169. Rzechowska E., Garbacz A., Majda M., Zaborek K., *Osoby 50+ na rynek pracy:* interementoring *jako element budowania dojrzałej współpracy międzypokoleniowej*.
170. Sarapata A. *Bodźce ekonomiczne w przedsiębiorstwie przemysłowym*. Warszawa: - PWE, 2008.
171. Sajkiewicz A., *Zasoby ludzkie w firmie. Organizacja, kierowanie, ekonomika*, Wydawnictwo Poltext, Warszawa 2004.
172. Sajkiewicz A., *Zasoby ludzkie w firmie. Organizacja, kierowanie, ekonomika*, Wydawnictwo Poltext, Warszawa 2000.
173. Schmidt J., *Rozwój organizacji pozarządowych. Teoria i praktyka*, Wydawnictwo Akademickie Sedno, Warszawa 2012.
174. Schumpeter J. A., *Teoria rozwoju gospodarczego*, Wydawnictwo Naukowe PWN, Warszawa 1960.
175. Sienkiewicz P., *Podstawy teorii systemów*, Wydawnictwo AON, Warszawa 1993.
176. Sienkiewicz P., *Teoria i inżynieria bezpieczeństwa systemów*, t. I, Zeszyty Naukowe AON, Warszawa 2007.
177. Sienkiewicz P., *Inżynieria systemów*, Wydawnictwo MON, Warszawa 1983.
178. Sienkiewicz P., Społeczeństwo informacyjne jako system cybernetyczny, Uczelniane Wydawnictwo Naukowo-Dydaktyczne, Kraków 2004.

179. Sirko S., *Procesy w organizacji*, Wydawnictwo Akademii Obrony Narodowej, Warszawa 2010.
180. Skoczylas J., *Prawo ratownicze, wydanie 2*, Lexis Nexis, Warszawa, 2011.
181. Smółka P., *Coaching. Inspiracje z perspektywy nauki, praktyki i klientów*, Wydawnictwo OnePress, Gliwice 2012.
182. Sołtysińska, M. Kossowska, *Szkolenia pracowników a rozwój organizacji*, Wydawnictwo Oficyna Ekonomiczna, Kraków 2002.
183. Sośnicki K., *Dydaktyka ogólna*, Wydawnictwo Księgarnia Naukowa, Toruń 1948.
184. Stabryła A., *Universal research approaches in designing development projects*, "Zeszyty Naukowe Małopolskiej Wyższej Ekonomicznej w Tarnowie" 2(19) (2011).
185. Stacewicz J., *Dylematy projektowania strategii i polityki rozwoju*, Wydawnictwo SGH, Warszawa 1998.
186. Stacewicz J., *W kierunku metaekonomicznej teorii i polityki rozwoju*, Wydawnictwo SGH - Prace i Materiały Instytutu Rozwoju Gospodarczego, 2002.
187. Stallings W., Kryptografia i bezpieczeństwo sieci komputerowych. Koncepcje i metody bezpiecznej komunikacji, Helion, Gliwice 2012.
188. Stańczyk J., *Współczesne pojmowanie bezpieczeństwa*, Wydawnictwo ISP PAN, Warszawa 1996.
189. Stefanowicz J., *Bezpieczeństwo współczesnych państw*, Wydawnictwo Instytut Wydawniczy PAX, Warszawa 1984.
190. Stefanowicz B., Informacja, SGH, Warszawa 2004.
191. Starr J., *Coaching*, Wydawnictwo Polskie Wydawnictwo Ekonomiczne, Warszawa 2005.
192. Sułek A., *Decyzje optymalne w badaniach stosowanych*, Wydawnictwo PWN, Warszawa 1979.
193. Szałkowski A., *Rozwój personelu*. - Kraków: AE, 2002.
194. Szczepanik R., *Outdoor z (ośmioma) zasadami* w: „Personel i Zarządzanie", nr 7.
195. Szczygieł A., *Identyfikacja potrzeb szkoleniowych w organizacji*. *UE w Krakowie*. Kraków: Katedra Psychologii i Dydaktyki, 2007.
196. Szewczyk R., Grela J., Bloch M., *Coaching zespołowy. Praktyczny przewodnik*, Wydawnictwo Helion, Gliwice 2020.
197. Strzoda M., Zarządzanie informacjami w organizacji, AON, Warszawa 2004.
198. Sutton R. J., Bezpieczeństwo telekomunikacji, przeł. G. Stawikowski, Wydawnictwo Komunikacji i Łączności, Warszawa 2004
199. Sztumski J., *Wstęp do metod i technik badań społecznych*, „Śląsk" Wydawnictwo Naukowe, 2010.
200. Szulc B., *Proces badań w naukach o obronności*, Praca naukowo-badawcza, Kod pracy: II.2.24.2., AON, Warszawa 2014.
201. Szymaniec P., *Heglowski model nowoczesnego państwa*, Zeszyty Naukowe Państwo-koncepcje i zadania, Uniwersytet Wrocławski.
202. Trawińska-Konador A., Sienkiewicz Ł., Chłoń-Domińczak A., *Zarządzanie zasobami ludzkimi w oparciu o kompetencje*.- Warszawa: Instytut Badań Edukacyjnych, 2013.
203. Urbaniak M., *Zarządzanie jakością*, Wydawnictwo Difin, Warszawa 2004.
204. Vickers A., Bavister S., *Coaching*, Wydawnictwo Helion, Gliwice 2007.
205. Warmiński A., *Zadania i organizacja Państwowej Straży Pożarnej w zakresie ochrony przeciwpożarowej*, Doctrina, Akademia Podlaska, Siedlce 2009.
206. Węgrzyn A., Benchmarking: *Nowoczesna metoda doskonalenia przedsiębiorstwa*, Wydawnictwo Antykwa, Wrocław 2000.
207. Wiśniewski E. S., *Metodyka wojskowych badań naukowych,* Wydawnictwo ASG WP, Warszawa 1990.

208. Witkowska M., Cholawo-Soszoch K., Społeczeństwo informacyjne. Istota, rozwój, wyzwania, WAiP, Warszawa 2006.
209. Whitfield R., *Innowacje w przemyśle*, Państwowe Wydawnictwo Ekonomiczne 1997.
210. Wołejszo J., *Formy i metody szkolenia dowództw wojsk lądowych*, Wydawnictwo Akademia Obrony Narodowej- Wydział Wydawniczy, Warszawa 2005.
211. Wołejszo J., *Proces szkolenia obronnego*, Wydawnictwo Kaliskie Towarzystwo Przyjaciół Nauk, Kalisz 2020.
212. Wołejszo J., *Wybrane aspekty doskonalenia ośrodków decyzyjnych*, Wydawnictwo AON, Warszawa 2003.
213. Wright McMahan, *Strategiczne zarządzanie personelem*, „Dziennik Zarządzania", czerwiec 1992.
214. Wrzosek M., *Identyfikacja zagrożeń organizacji zhierarchizowanej*, Wyd. Akademii Obrony Narodowej, Warszawa 2010.
215. Zajączkowska A., Gałusa H., Gotowczyc A., *Vademecum Mentoringu wiedza w pigułce*, Wydawnictwo Fundacja Forum Mentorów AHA EFFECT, Gdańsk 2016.
216. Zimmermann J., *Prawo administracyjne*, Wolters Kluwer, Warszawa 2014.
217. Zieleniewski J., *Organizacja i zarządzanie*, Wydawnictwo PWE, Warszawa 1979.
218. Żebrowski A., *Walka informacyjna u progu XXI wieku*, [w:] Borowiecki R., Romantowska M. (red.), *System informacji strategicznej. Wywiad gospodarczy a konkurencyjność przedsiębiorstwa*, Wydawnictwo Dyfin, Warszawa 2001.
219. Żegnałek K., *Metody i techniki stosowane w badaniach pedagogicznych*, Wydawnictwo Wyższej Szkoły Pedagogicznej Towarzystwa Wiedzy Powszechnej, Warszawa 2008.
220. Żuber vel Michałowski J., *Prawne umocowanie systemu*, „Przegląd Pożarniczy" 1995.
221. Żukrowska K., Gracik M., Bezpieczeństwo międzynarodowe, Wydawnictwo SGH, Warszawa 2006.

Akty prawne

1. Ustawa z dnia 24 sierpnia 1991 r. o ochronie przeciwpożarowej t.j (Dz.U. z 2022 r., poz. 2057)
2. Ustawa z dnia 24 sierpnia o 1991 r. Państwowej Straży Pożarnej t.j. (Dz.U. z 2022 r., poz. 1969, ze zm.).
3. Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym t.j. (Dz.U. z 2023 r., poz. 122).
4. Ustawa z dnia 5 czerwca 1998 r. o samorządzie powiatowym t.j. (Dz.U. z 2022 r., poz. 1526, ze zm.).
5. Ustawa z dnia 8 marca 1990 r. o samorządzie gminnym t.j. (Dz.U. z 2023 r., poz. 40, ze zm.)
6. Ustawa z dnia 8 marca 1990 r. o samorządzie województwa (Dz.U. z 2022 r., poz. 2094, ze zm.).
7. Ustawa z dnia 5 sierpnia 2010 roku o ochronie informacji niejawnych, Dz. U. 2010,
8. Nr 182, poz. 1228 (t.j. Dz. U. z 2019 r., poz. 742 z późn. zm.).
9. Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 3 lipca 2017 r. w sprawie szczegółowych zasad organizacji krajowego systemu ratowniczo-gaśniczego (Dz. U. z 2017 r., poz. 1319 ze zm.).
10. Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 21 listopada 2014 r. w sprawie szczegółowych zasad wyposażenia jednostek organizacyjnych Państwowej Straży Pożarnej (Dz. U. z 2014, poz. 1793).

Akty normatywne

1. PN-ISO/IEC 17799:2007

Linki do stron internetowych

1. https://mfiles.pl/pl/index.php/Cechy_informacji, Encyklopedia zarządzania
2. https://sjp.pwn.pl/slowniki/niespójność.html
3. https://pl.linkedin.com/pulse/czym-jest-skuteczność-efektywność-działań-miłosz-mróz
4. https://www.projektprzywodztwo.com/otoczenie-organizacji
5. https://sites.google.com/site/szostokkomunikacja/swdsd
6. https://sjp.pwn.pl/
7. https://cyberdefence24.pl
8. https://www.zabezpieczenia.com.pl/ochrona-informacji/system-zarządzaniabezpieczeństwem-informacji-zgodny-z-isoiec-27001-cz-1
9. http://sjp.pwn.pl/sjp/informacja
10. http://synonim.net/synonim/informacja,
11. https://www.mbridge.pl/szum-informacyjny-czym-jest/
12. https://sjp.pwn.pl/slowniki/chaotyczny.html
13. https://www.znak.com.pl/ksiazka/ekologia-informacji-wieslaw-babik-69581
14. http://www.pg.gda.pl/~krzyte/students/1. Analiza elementów komunikacji.
15. https://poradnikprzedsiebiorcy.pl
16. https://mfiles.pl/pl/index.php/Polityka_bezpieczeństwa, Encyklopedia Zarządzania

Spis rysunków

Spis Tabel

SPIS WYKRESÓW

ZAŁĄCZNIK nr 1 - KWESTIONARIUSZ ANKIETY

Kwestionariusz Ankiety

Ankieta posiada charakter jednokrotnego wyboru. Dziękuję za poświęcony czas.

Metryczka:

Wiek

- **Do 25 lat**
- **26-35 lat**
- **36-45 lat**
- **46 lat i więcej**

Staż służby

- **Do 10 lat**
- **11-20 lat**
- **21-30**
- **31 lat i więcej**

Wykształcenie

- **Podstawowe**
- **Średnie**
- **Wyższe**

Miejsce zatrudnienia

- **Komenda Wojewódzka**
- **Komenda Powiatowa/Miejska**

1. **Czy uważa Pani/Pan, że system informacyjny (system wymiany informacji) ma strategiczny wpływ na funkcjonowanie jednostki macierzystej i całej organizacji PSP?**

a) **tak**
b) **nie**
c) **trudno powiedzieć**

2. **Czy uważa Pani/Pan, że zapewnienie bezpieczeństwa systemu informacyjnego (identyfikacja zagrożeń i możliwych usprawnień) jest podstawowym zadaniem instytucji publicznej w dzisiejszych czasach?**

a) **tak**
b) **nie**
c) **trudno powiedzieć**

3. **Które z wymienionych poniżej podstawowych zasobów ma Pani/Pana zdaniem największy wpływ na skuteczne funkcjonowanie organizacji?**

a) **ludzie (wiedza, umiejętności zdolności)**
b) **struktura organizacyjna**
c) **system informacyjny (informacje będące w posiadaniu instytucji)**
d) **zasoby rzeczowe (sprzęt, narzędzia, maszyny)**

4. **Czy w Pani/Pana jednostce wprowadzone są procedury, regulaminy i instrukcje – polityka bezpieczeństwa informacji?**

a) **tak**
b) **nie**
c) **nie wiem**

5. **Która z niżej wymienionych form komunikacji w Pani/Pana macierzystej jednostce PSP jest najskuteczniejsza?**

a) **odprawy/narady służbowe**
b) **pisma tradycyjne**
c) **tablice ogłoszeń**
d) **łączność telefoniczna**
e) **systemy elektroniczne (wideokonferencyjne i internetowe)**

6. Która z poniższych cech informacji Pani/Pana zdaniem jest najważniejsza/ ma największy wpływ na skuteczne funkcjonowanie organizacji?

a) dostępność – możliwość uzyskania właściwej kategorii informacji
b) poufność – zabezpieczenie przed dostępem osób nieupoważnionych
c) aktualność – dostępna w czasie pozwalającym na podjęcie decyzji
d) niezawodność – odzwierciedlająca rzeczywistość
e) kompletność – dostarcza największa ilość faktów i szczegółów
f) użyteczność - otrzymywane informacje mają znaczenie dla odbiorcy i są dla niego użyteczne
g) wszystkie powyżej

7. Który z niżej wymienionych elementów komunikacji uważa Pani/Pan za najczęściej spotykany błąd w PSP?

a) przełożeni wymagają zbyt wiele i nie reagują na sugestie podwładnych
b) przekazywane informacje są często niezrozumiałe dla adresata
c) przekazywane wiadomości zawierają zbyt wiele danych interesujących kierownictwo, a nie pracowników
d) komunikaty są za oficjalne, w jednostce jest zbyt mało otwartości i szczerości

8. Czy według Pani/Pan system informacyjny PSP w pełni chroni informacje pozyskiwane i przetwarzane przez tą formację?

a) tak
b) częściowo tak, ale wymaga ciągłego udoskonalania
c) nie
d) trudno powiedzieć

9. Które z niżej wymienionych zagrożeń jest Pani/Pan zdaniem najpoważniejsze dla systemu informacyjnego w PSP?

a) ludzie i ich działania (świadome, bądź nieświadome)
b) klęski żywiołowe (pożar, katastrofy techniczne, zalanie pomieszczeń, itp.)
c) wady techniczne sprzętu
d) cyberatak w tym wirusy, robaki, konie trojańskie
e) przekazywanie informacji osobom nieuprawnionym

10. Czy posiada Pani/Pan świadomość konsekwencji o skutkach łamania zasad korzystania z systemu informacyjnego PSP i braku odpowiedzialności?

a) tak

b) nie

c) nie zapoznano mnie z nimi

11. Który z niżej wymienionych elementów Pani/Pana zdaniem ma decydujący wpływ na bezpieczeństwo systemu informacyjnego w PSP?

a) wprowadzenie właściwych rozwiązań organizacyjnych (polityka bezpieczeństwa)

b) rzetelne szkolenia dla funkcjonariuszy i pracowników

c) bieżąca kontrola i nadzór

d) wprowadzenie właściwych zabezpieczeń technicznych

e) wszystkie powyżej

12. Czy przyjęty w Pani/Pana macierzystej jednostce system obiegu informacji spełnia oczekiwania funkcjonalne?

a) tak

b) nie

c) należy go usprawnić

d) nie mam zdania

13. Który z przedstawionych poniżej czynników Pani/Pana zdaniem wpływa najbardziej na niedoskonałość systemu informacyjnego w PSP?

a) rozbudowana struktura organizacyjna

b) brak rozwiązań, zabezpieczeń technologicznych

c) brak dokładnych i rzetelnych informacji

d) brak szkoleń w zakresie systemu informacyjnego

e) system informacyjny jest sprawny i nie potrzebuje ulepszeń

14. Czy Pani/Pana zdaniem funkcjonujący w jednostce system szkoleń w zakresie systemu informacyjnego i jego bezpieczeństwa jest właściwy?

a) tak, posiadam wszystkie niezbędne informacje w tym zakresie

b) nie, uważam że pracodawca powinien zapewnić mi większy zasób informacji w tym zakresie

c) trudno powiedzieć

15. Które z poniższych działań Pani/Pana zadaniem mogą poprawić skuteczność funkcjonowania systemu informacyjnego w PSP?

a) spłaszczenie struktury organizacyjnej jednostki

b) selekcja informacji w celu wyeliminowania informacji nieprzydatnych

c) bieżące badanie potrzeb informacyjnych użytkowników pod kątem ich oczekiwań

d) ograniczenie korespondencji papierowej na rzecz elektronicznego przekazu informacji

16. Czy według Pana/Pani pełne ujednolicenie systemów teleinformatycznych na wszystkich poziomach organizacyjnych PSP zwiększyłoby efektywność bezpieczeństwa systemu informacyjnego?

a) zdecydowanie tak

b) w pewnym stopniu

c) raczej nie

d) nie miałoby to w ogóle wpływu na poprawę systemu

17. Czy Pani/Pana zdaniem zasadnym jest wyodrębnienie w macierzystej jednostce stanowiska/osoby odpowiedzialnej za przekazywanie informacji od kierownictwa do szczebla wykonawczego oraz zbieranie i przekazywanie informacji zwrotnych?

a) tak, usprawni to przepływ informacji

b) nie, nie będzie miało to wpływu na przepływ informacji

c) nie mam zdania

d) taka osoba/stanowisko istnieje już w mojej jednostce macierzystej

18. Czy Pani/Pana zdaniem budowa chmury obliczeniowej dla PSP, tzn. dostarczanie przez Internet kluczowych usług obliczeniowych - w tym serwerów, pamięci masowej, baz danych i oprogramowania znacząco wpłynęłoby na poprawę funkcjonowania systemu informacyjnego?

a) **tak**
b) **nie**
c) **nie wiem**

19. Czy Pani/Pana zdaniem migracja usług systemów łączności radiowej z analogowych do cyfrowych jest dobrym kierunkiem?

a) **tak**
b) **nie**
c) **nie wiem**

20. Czy Pani/Pana zdaniem zmiana architektury Systemu Wspomagania Decyzji PSP z rozproszonej na scentralizowaną oraz dodanie nowych modułów (m in. współpracy z jednostkami Ochotniczych Straży Pożarnych, współpracy z innymi instytucjami współdziałającymi) usprawni procesy obsługi zdarzeń?

a) **tak**
b) **nie**
c) **nie wiem**

ZAŁĄCZNIK nr 2 – ARKUSZ OBSERWACJI

ARKUSZ OBSERWACJI
SYSTEMU WYMIANY INFORMACJI W PAŃSTWOWEJ STRAŻY POŻARNEJ

1. TEMAT BADAŃ: Tematem badań jest system bezpieczeństwa wymiany informacji w Państwowej Straży Pożarnej.

2. ZASTOSOWANE METODY BADAWCZE: Obserwacja niestandaryzowana zewnętrzna (postronna) oraz wewnętrzna (uczestnicząca).

3. CEL BADAŃ: Identyfikacja występujących zagrożeń i możliwych usprawnień w systemie bezpieczeństwa informacji w Państwowej Straży Pożarnej jako organizacji publicznej (zhierarchizowanej).

4. CZAS BADAŃ: marzec 2022 – maj 2023 r.

5. OPIS PRZEBIEGU BADAŃ: Do przeprowadzenia badań użyto metody obserwacji niestandaryzowanej zewnętrznej (postronnej) oraz wewnętrznej (uczestniczącej).

Podczas obserwacji niestandaryzowanej zewnętrznej autor posługiwał się podejściem badawczym, które polegało na bezpośrednim obserwowaniu i dokumentowaniu zachowań, sytuacji, zjawisk w naturalnym środowisku służby funkcjonariuszy PSP - bez ingerencji badacza.

Pozwoliło to na zbieranie danych w realistycznych warunkach, w których badani zachowywali się naturalnie. Autor badań uzyskał tym samym bogatych, szczegółowych danych o zachowaniu jednostek w ich naturalnym otoczeniu, co pozwoliło na lepsze zrozumienie kontekstu i czynników wpływających na zachowanie badanych osób w kontekście bezpieczeństwa systemu informacyjnego.

Metoda obserwacji wewnętrznej uczestniczącej polegała na aktywnym uczestnictwie badacza w badanym środowisku, gdzie stawał się on częścią grupy lub społeczności, którą obserwował i czynnie uczestniczył w jej codziennych działaniach.

W tej metodzie badacz starał się zrozumieć badane zjawisko poprzez doświadczenie go osobiście i zdobycie wglądu wewnętrznego. Przebywanie w grupie badanej umożliwiło obserwację i analizę interakcji, norm, wartości, hierarchii społecznej oraz innych istotnych aspektów dotyczących funkcjonowania systemu bezpieczeństwa informacyjnego w PSP. Metoda ta używana była podczas odpraw służbowych z kadrą kierowniczą, ale także podczas bieżącego kontaktu z funkcjonariuszami pełniącymi służbę na stanowiskach wyko-

nawczych. Dało to możliwość do wymiany poglądów, opinii i spostrzeżeń nie tylko z funkcjonariuszami odpowiedzialnymi za przekazywanie informacji w pionie, na niższe szczeble, ale również na zapoznanie się z poziomem przyswojenia informacji dotyczących bezpieczeństwa systemu informacyjnego przez funkcjonariuszy, do których były one bezpośrednio kierowane.

W oparciu o wyniki prowadzonych obserwacji ich autor sformułował w odniesieniu do problematyki systemu bezpieczeństwa informacyjnego Państwowej Straży Pożarnej następujące wnioski:

1. Wykonując swoje zadania Państwowa Straż Pożarna jako instytucja publiczna, posiada swój system bezpieczeństwa wymiany informacji, w którym można zaobserwować trudności i problemy, które bez wątpienia mają wpływ na bezpieczeństwo obiegu informacji wewnątrz instytucji. Bezpieczeństwo systemu informacyjnego powinno zatem obejmować środowisko techniczne, informatyczne, system zarządzania, ekonomikę organizacji, zasoby ludzkie, otoczenie prawne i społeczne.
2. Realizacja coraz większej liczby zadań postawionych przed administracją państwa, związana jest z koniecznością wykorzystania nowoczesnych technologii oraz systemów teleinformatycznych, co wymaga przetwarzania dużej ilości zbiorów danych. Państwowa Straż Pożarna funkcjonuje w środowisku zwiększonej ilość informacji, rozwoju informatyzacji, konieczności ułatwiania dostępu do danych, usprawnienie procesów przekazywania lub pobierania ich znacznych ilości w niewielkich jednostkach czasu. Tylko takie podejście pozwala odpowiednio przygotować się na zakłócenia związane z brakiem dostępności i integralności lub utratą poufności danych itp.
3. W Państwowej Straży Pożarnej przetwarzane są również informacje niejawne oraz gromadzą są dane archiwalne. Bezpieczeństwo informacji z racji ilości, różnorodności oraz ważności realizowanych przez tą instytucję zadań jest ważna dla całego społeczeństwa. Złożoność procesu pozyskiwania, gromadzenia, utrzymywania, aktualizowania, przetwarzania, przesyłania i archiwizowania informacji wymaga szczególnych, systemowych form postępowania na każdym jej etapie.
4. Kierownik każdej jednostki organizacyjnej PSP winien propagować politykę bezpieczeństwa informacyjnego wśród swojej kadry. Racjonalność w zarządzaniu informacją zaświadcza o wysokich kompetencjach menedżerskich oraz jest synonimem podążania jednostki za nieustannym rozwojem, który wywołuje ciągłą zmienność potrzeb.
5. Uwzględniając różne predyspozycje zarówno nadawców informacji jak i ich odbiorców,

konieczne jest dostosowanie sposobu ich przekazu do posiadanych umiejętności i zastosowanie właściwych technik przekazu werbalnego np. forma mówiona, pisemna, graficzna.

6. Dzisiejsza rzeczywistość zmusza do wnikliwej analizy poziomu bezpieczeństwa systemu informacyjnego w podmiotach sfery publicznej, tak aby nadążać za pojawiającymi się zagrożeniami. Dodatkowym czynnikiem determinującym potrzebę zainteresowania przedmiotową tematyką bezpieczeństwa informacji są potrzeby dostosowywania organizacji do wymagań mających zastosowanie przepisów prawa i innych wymagań, których celem jest zapewnienie ochrony określonym grupom interesariuszy.
7. Dynamiczne zmiany aktów prawnych, ustaw, rozporządzeń, zarządzeń i wytycznych, ale także stanowisk i interpretacji prawnych obowiązujących przepisów, determinują konieczność ich poszukiwania w dostępnych źródłach. Zatem niezwykle istotnym elementem uzyskiwania informacji jest samokształcenie się funkcjonariuszy na każdym szczeblu struktury organizacyjnej i dzielenie się zdobytą wiedzą. Rozwój poszczególnych funkcjonariuszy ma ogromny wpływ na rozwój całej formacji i jest jednym z czynników nowoczesnego zarządzania.
8. Uwzględniając potrzeby poszczególnych funkcjonariuszy w obszarze przepływu informacji, zachowując jednak konieczność hierarchiczność struktury organizacyjnej Państwowej Straży Pożarnej w kontekście przepływu informacji w górę i w dół struktury organizacyjnej, należy stworzyć funkcjonariuszom warunki do tego, aby ich głos był zauważalny, a przede wszystkim kierownictwo wsłuchiwało się w głos podwładnych. Tylko przy zachowaniu tego warunku możliwe jest uzyskanie odpowiednich informacji i ich zgromadzenie.

Dlatego dogłębne poznanie przedmiotu badań jakim jest bezpieczeństwo systemu informacyjnego Państwowej Straży Pożarnej, jako organizacji publicznej winno mieć przełożenie na właściwą organizację jej struktury poprzez skuteczne zarządzanie bezpieczeństwem informacyjnym. W ocenie badającego bezpieczeństwo systemu informacyjnego bez wątpienia ma istotny wpływ na zapewnienie bezpieczeństwa narodowego, a problematyka bezpieczeństwa systemu informacyjnego powinna być nadrzędnym celem w zarządzaniu, każdą organizacją.