

Publikacja współfinansowana ze środków Unii Europejskiej w ramach Europejskiego Funduszu Społecznego

**Rozwijanie, uzupełnianie i aktualizacja informacji o zawodach oraz jej upowszechnianie
za pomocą nowoczesnych narzędzi komunikacji – INFODORADCA+**

INFORMACJA O ZAWODZIE

Specjalista do spraw systemów zarządzania bezpieczeństwem informacji (252903)



**Specjaliści do spraw baz danych i sieci komputerowych
gdzie indziej niesklasyfikowani**

**Rozwijanie, uzupełnianie i aktualizacja informacji o zawodach oraz jej rozpowszechnianie
za pomocą nowoczesnych narzędzi komunikacji – INFODORADCA+**

Projekt jest współfinansowany ze środków Unii Europejskiej w ramach Europejskiego Funduszu Społecznego

INFORMACJA O ZAWODZIE

Specjalista do spraw systemów zarządzania bezpieczeństwem informacji

(252903)

**Specjaliści do spraw baz danych i sieci komputerowych
gdzie indziej niesklasyfikowani**

Ministerstwo Rodziny, Pracy i Polityki Społecznej, Departament Rynku Pracy

Publikacja opracowana w ramach projektu **Rozwijanie, uzupełnianie i aktualizacja informacji o zawodach oraz jej upowszechnianie za pomocą nowoczesnych narzędzi komunikacji – INFODORADCA+**

Program Operacyjny Wiedza Edukacja Rozwój, Oś priorytetowa II Efektywne polityki publiczne dla rynku pracy, gospodarki i edukacji, Działanie 2.4 Modernizacja publicznych i niepublicznych służb zatrudnienia oraz lepsze dostosowanie ich do potrzeb rynku pracy

PROJEKT NR: POWR.02.04.00-00-0060/16-00

Partnerzy projektu INFODORADCA+:

- DORADCA Consultants Ltd Sp. z o.o., Gdynia
- Instytut Technologii Eksploatacji – Państwowy Instytut Badawczy, Radom
- Instytut Pracy i Spraw Socjalnych, Warszawa
- Centralny Instytut Ochrony Pracy – Państwowy Instytut Badawczy, Warszawa
- PBS Sp. z o.o., Sopot

INFORMACJA O ZAWODZIE

Specjalista do spraw systemów zarządzania bezpieczeństwem informacji (252903)

© Ministerstwo Rodziny, Pracy i Polityki Społecznej, Departament Rynku Pracy, Warszawa 2018

Kopiowanie i rozpowszechnianie w całości lub w części dozwolone wyłącznie za podaniem źródła.

ISBN 978-83-7789-495-8 [184]

Publikacja bezpłatna

Zdjęcie na okładce (źródło): <https://pixabay.com/pl/bezpiecze%C5%84stwo-cybernetyczne-2776600>
[dostęp: 31.10.2018].



SPIS TREŚCI

1. DANE IDENTYFIKACYJNE ZAWODU	3
1.1. Nazwa i kod zawodu (wg Klasyfikacji zawodów i specjalności).....	3
1.2. Nazwy zwyczajowe zawodu.....	3
1.3. Usytuowanie zawodu w klasyfikacjach: ISCO, PKD	3
1.4. Notka metodologiczna, autorzy i eksperci opiniujący	3
2. OPIS ZAWODU.....	4
2.1. Synteza zawodu	4
2.2. Opis pracy i sposobu jej wykonywania	4
2.3. Środowisko pracy (warunki pracy, maszyny i narzędzia pracy, zagrożenia, organizacja pracy).....	5
2.4. Wymagania psychofizyczne i zdrowotne.....	6
2.5. Wykształcenie, tytuły zawodowe, kwalifikacje i uprawnienia niezbędne/preferowane do podjęcia pracy w zawodzie.....	7
2.6. Możliwości rozwoju zawodowego, awansu i potwierdzania kompetencji	8
2.7. Zawody pokrewne	9
3. ZADANIA ZAWODOWE I WYMAGANE KOMPETENCJE	9
3.1. Zadania zawodowe	9
3.2. Kompetencja zawodowa Kz1: Pozyskiwanie, weryfikowanie i przechowywanie informacji	9
3.3. Kompetencja zawodowa Kz2: Zarządzanie systemem bezpieczeństwa informacji	11
3.4. Kompetencja zawodowa Kz3: Wdrażanie, nadzorowanie i aktualizowanie systemu zarządzania bezpieczeństwem informacji	12
3.5. Kompetencje społeczne.....	13
3.6. Profil kompetencji kluczowych dla zawodu.....	13
3.7. Powiązanie kompetencji zawodowych z opisami poziomów Polskiej Ramy Kwalifikacji oraz Sektorowej Ramy Kwalifikacji.....	14
4. ODNIESIENIE DO SYTUACJI ZAWODU NA RYNKU PRACY I MOŻLIWOŚCI DOSKONALENIA ZAWODOWEGO.....	14
4.1. Możliwości podjęcia pracy w zawodzie	14
4.2. Instytucje oferujące kształcenie, szkolenie i/lub potwierdzanie kompetencji w ramach zawodu	15
4.3. Zarobki osób wykonujących dany zawód/daną grupę zawodów	16
4.4. Możliwości zatrudnienia osób niepełnosprawnych w zawodzie.....	17
5. ODNIESIENIE DO EUROPEJSKIEJ KLASYFIKACJI UMIEJĘTNOŚCI/KOMPETENCJI, KWALIFIKACJI I ZAWODÓW (ESCO)	17
6. ŹRÓDŁA DODATKOWYCH INFORMACJI O ZAWODZIE	18
7. SŁOWNIK POJĘĆ	19
7.1. Definicje powiązane z opisem informacji o zawodzie (zawodoznawcze)	19
7.2. Definicje związane z wykonywaniem zawodu (branżowe)	22

1. DANE IDENTYFIKACYJNE ZAWODU

1.1. Nazwa i kod zawodu (wg Klasyfikacji zawodów i specjalności)

Specjalista do spraw systemów zarządzania bezpieczeństwem informacji 252903

1.2. Nazwy zwyczajowe zawodu

- Administrator bezpieczeństwa informacji.
- Audytor do spraw bezpieczeństwa informacji.
- Audytor wewnętrzny do spraw systemów zarządzania bezpieczeństwem informacji.
- Menedżer bezpieczeństwa informacji.
- Pełnomocnik do spraw systemu zarządzania bezpieczeństwem informacji.
- Specjalista ds. bezpieczeństwa informacji.

1.3. Usytuowanie zawodu w klasyfikacjach: ISCO, PKD

W Międzynarodowym Standardzie Klasyfikacji Zawodów ISCO-08 odpowiada grupie:

- 2529 Database and network professionals not elsewhere classified.

Według Polskiej Klasyfikacji Działalności (PKD 2007):

- Sekcja J – Informacja i komunikacja.

1.4. Notka metodologiczna, autorzy i eksperci opiniujący

Notka metodologiczna

Opis informacji o zawodzie opracowano na podstawie:

- analizy źródeł (akty prawne, klasyfikacje krajowe, międzynarodowe) oraz źródeł internetowych,
- analizy opisu zawodu zamieszczonego w wyszukiwarce opisów zawodów na Portalu Publicznych Służb Zatrudnienia,
- badań ankietowych prowadzonych w projekcie INFODORADCA+ w listopadzie 2018 r.,
- zebranych opinii od recenzentów, członków panelu ewaluacyjnego oraz zespołu ds. walidacji i jakości informacji o zawodach.

Autorzy i eksperci opiniujący

Zespół Ekspercki:

- Jakub Bieszke – HS PARTNER Jakub Bieszke, Gdańsk.
- Michał Filipowski – FilCon Inf Michał Filipowski, Dębogórze.
- Włodzimierz Walkusz – DORADCA Consultants Ltd. Sp. z o.o., Gdynia.

Zespół ds. walidacji i jakości informacji o zawodzie:

- Anna Będzińska – DORADCA Consultants Ltd. Sp. z o.o., Gdynia.
- Wojciech Gostomski – DORADCA Consultants Ltd. Sp. z o.o., Gdynia.
- Joanna Gralak-Merchel – DORADCA Consultants Ltd. Sp. z o.o., Gdynia.
- Jolanta Religa – Instytut Technologii Eksploatacji – PIB, Radom.
- Krzysztof Symela – Instytut Technologii Eksploatacji – PIB, Radom.

Recenzenci:

- Damian Rusek – RADMOT Sp. z o.o. Sp.k., Radom.
- Dariusz Tomczak – Zespół Szkół Elektrycznych im. prof. Janusza Groszkowskiego w Białymstoku, Białystok.

Panel ewaluacyjny – przedstawiciele partnerów społecznych:

- Bernard Kubiak – Wyższa Szkoła Administracji i Biznesu w Gdyni, Gdynia.
- Radosław Niemczewski – Centrum Kształcenia Praktycznego, Pleszew.

Data (rok) opracowania opisu informacji o zawodzie: 2018 r.

WAŻNE:

W tekście opisu informacji o zawodzie występują podkreślenia wybranych określeń wraz z indeksem górnym, który wskazuje numer definicji w słowniku branżowym w punkcie 7.2.

2. OPIS ZAWODU

2.1. Synteza zawodu

Specjalista do spraw systemów zarządzania bezpieczeństwem informacji⁸ jest odpowiedzialny za projektowanie, wdrożenie, nadzór i doskonalenie zarządzania zasobami technicznymi i organizacyjnymi zapewniającymi ochronę bezpieczeństwa każdej informacji zidentyfikowanej w przedsiębiorstwie. Osoba wykonująca ten zawód może także udzielać wsparcia technicznego i organizacyjnego dla certyfikowanych audytorów¹ zintegrowanych systemów zarządzania bezpieczeństwem informacji, zgodnie z przyjętymi normami jakości¹⁴.

2.2. Opis pracy i sposobu jej wykonywania

Opis pracy

Specjalista do spraw systemów zarządzania bezpieczeństwem informacji realizuje zadania związane z zapewnieniem bezpieczeństwa informacji w organizacji. Zajmuje samodzielne stanowisko bezpośrednio zależne i nadzorowane przez kluczowe osoby w organizacji lub właściciela przedsiębiorstwa. Odpowiedzialny jest za projektowanie procesów¹⁸ wewnętrznych i procedur, które zapewniają dostępność informacji i danych poufnych³ tylko dla osób uprawnionych¹⁵.

Specjalista do spraw systemów zarządzania bezpieczeństwem informacji odpowiednio przechowuje, przetwarza, integruje oraz zapewnia upoważnionym użytkownikom dostęp do informacji i związanych z nimi zasobów. Dysponuje poufnymi danymi firmy, które wymuszają nadzór, dodatkowe monitorowanie i optymalizację działania pracowników w celu poprawy bezpieczeństwa informacji w organizacji.

Sposoby wykonywania pracy

W swojej pracy **specjalista do spraw systemów zarządzania bezpieczeństwem informacji** stosuje metody, techniki i procedury związane m.in. z:

- opracowywaniem i monitorowaniem przestrzegania polityki bezpieczeństwa¹⁷ informacji,
- doradzaniem pracownikom organizacji w zakresie bezpieczeństwa informatycznego – w dużych organizacjach większość czasu pracy poświęca bieżącemu doradztwu telefonicznemu, mailowemu lub osobistemu,
- monitorowaniem informacji, przypisywaniem im klauzuli poufności¹² oraz zarządzaniem danymi, tworzącymi spójny system zarządzania bezpieczeństwem informacji,
- utrzymywaniem planów odtwarzania informacji po nieprzewidzianych incydentach⁷,
- wspieraniem kierownictwa w monitorowaniu procesów biznesowych, prowadzeniem kontroli wewnętrznych i wdrażaniem środków zapobiegawczych w przypadku naruszenia bezpieczeństwa informacji,
- przeprowadzaniem symulowanych naruszeń systemu bezpieczeństwa,

- sprawozdawczością dla kierownictwa organizacji z realizacji polityki bezpieczeństwa oraz przedstawianiem propozycji wdrożenia środków zaradczych w przypadku jej naruszenia.

Specjalista do spraw systemów zarządzania bezpieczeństwem informacji może także:

- wykonywać prace analityczne w dziale IT⁴,
- brać udział w opracowaniu strategii informacyjnej przedsiębiorstwa²² w obszarze bezpieczeństwa informacji,
- reprezentować organizację na zewnątrz jako pełnomocnik kierownictwa do spraw zabezpieczeń i właściciel polityki bezpieczeństwa.

Więcej szczegółowych informacji znajduje się w sekcjach: 3.1. Zadania zawodowe oraz 3.2., 3.3. i 3.4. Kompetencje zawodowe.

2.3. Środowisko pracy (warunki pracy, maszyny i narzędzia pracy, zagrożenia, organizacja pracy)

Warunki pracy

Specjalista do spraw systemów zarządzania bezpieczeństwem informacji pracuje w pomieszczeniach biurowych, serwerowniach, różnego rodzaju archiwach. Są to pomieszczenia strzeżone, zlokalizowane z reguły w budynkach zatrudniającej go instytucji.

Praca odbywa się często w pomieszczeniach zamkniętych o dużym natężeniu hałasu, klimatyzowanych, ze sztucznym oświetleniem.

Więcej informacji znajduje się w sekcji: 4.1. Możliwości podjęcia pracy w zawodzie.

Wykorzystywane maszyny i narzędzia pracy

Specjalista do spraw systemów zarządzania bezpieczeństwem informacji w działalności zawodowej wykorzystuje m.in.:

- narzędzia informatyczne:
 - komputer wraz z aplikacjami biurowymi i specjalistycznymi oraz dostępem do internetu,
 - urządzenia wspomagające, w tym drukarki, kserokopiarki, skanery, projektory oraz inne urządzenia biurowe,
 - urządzenia sieciowe: serwery, routery²¹,
 - urządzenia mobilne: laptopy, tablety, telefony;
- narzędzia produkcyjne i infrastrukturalne:
 - czujniki produkcyjne²,
 - urządzenia do wzorcowania przyrządów,
 - sejfy, tajne pomieszczenia itp.

Organizacja pracy

Praca w zawodzie **specjalista do spraw systemów zarządzania bezpieczeństwem informacji** ma charakter ściśle umysłowy. Może być wykonywana samodzielnie lub w zespołach zadaniowych, w zależności od wielkości i potrzeb organizacji.

Specjalista do spraw systemów zarządzania bezpieczeństwem informacji może współpracować z pracownikami odpowiedzialnymi za nadzór powierzonych zadań w ramach systemu zarządzania bezpieczeństwem informacji oraz z zewnętrzną jednostką certyfikującą system zarządzania bezpieczeństwem informacji. Wnioski z kontroli przekazywane są ściślemu kierownictwu przedsiębiorstwa, które weryfikuje je z założonym planem polityki bezpieczeństwa.

Czas pracy jest najczęściej stały i w ramach formuły pracy etatowej nie przekracza normy 40 godzin w tygodniu, chociaż w małych organizacjach może funkcjonować w oparciu o zadaniowy system

pracy²⁷. Specjalista do spraw systemów zarządzania bezpieczeństwem informacji może pracować także jako zewnętrzny wykonawca usług (outsourcing¹⁶).

Wysokiej klasy specjaliści w zawodzie mogą pracować dla kilku organizacji – w takim modelu rozliczani są za utrzymanie bezpieczeństwa i certyfikacji dotyczącej zarządzania systemem bezpieczeństwa informacji.

Część zadań zawodowych jest możliwa do wykonywania w trybie zdalnym (telepraca²⁴).

Zagrożenia mające wpływ na bezpieczeństwo pracy człowieka

Typowymi zagrożeniami w zawodzie **specjalista do spraw systemów zarządzania bezpieczeństwem informacji** są m.in.:

- nadmierne obciążenia wzroku wynikające z długotrwałej pracy przy komputerze, w zamkniętych pomieszczeniach ze sztucznym oświetleniem,
- nadmierne obciążenie słuchu przy podwyższonym poziomie hałasu urządzeń serwerowych,
- przeciążenie układu kostno-szkieletowego związane z pracą w pozycji siedzącej – skrzywienia kręgosłupa (kifoza, lordoza), dyskopatia, zespół cieśni nadgarstka, łokieć tenisisty,
- stres, w przypadku trudnych relacji z użytkownikami, presji czasowej w zachowaniu przyjętych terminów realizacji powierzonych zadań lub trudnych relacji z audytorami instytucji certyfikującej system zarządzania.

2.4. Wymagania psychofizyczne i zdrowotne

Wymagania psychofizyczne

Dla pracownika wykonującego zawód **specjalista do spraw systemów zarządzania bezpieczeństwem informacji** ważne są:

w kategorii wymagań fizycznych

- ogólna wydolność fizyczna,
- sprawność narządu wzroku,
- sprawność narządu słuchu,
- sprawność układu kostno-stawowego;

w kategorii sprawności sensomotorycznych

- spostrzegawczość,
- koordynacja wzrokowo-słuchowa,
- ostrość wzroku,
- ostrość słuchu,
- rozróżnianie barw,
- zręczność rąk i palców,

w kategorii sprawności i zdolności

- uzdolnienia informatyczne,
- zdolność koncentracji uwagi,
- dobra pamięć,
- zdolność łatwego kojarzenia faktów i rozpoznawania schematów,
- zdolność analizowania i systematyzowania złożonych problemów,
- zdolność do przestrzegania reguł, przepisów i standardów,
- zdolność skutecznego przekonywania,
- dobra organizacja pracy własnej;

w kategorii cech osobowościowych

- zainteresowania informatyczne,

- zainteresowania techniczne,
- rzetelność,
- dokładność,
- samodzielność,
- systematyczność,
- samokontrola,
- odpowiedzialność,
- radzenie sobie ze stresem,
- komunikatywność,
- niezależność,
- gotowość do ustawicznego uczenia się,
- gotowość do wprowadzania zmian,
- zamiłowanie do ładu i porządku.

Więcej informacji znajduje się w sekcjach: 3.5. Kompetencje społeczne; 3.6. Profil kompetencji kluczowych dla zawodu.

Wymagania zdrowotne

Praca w zawodzie **specjalista do spraw systemów zarządzania bezpieczeństwem informacji** pod względem wydatku energetycznego należy do prac lekkich. W pracy występują specyficzne obciążenia umysłowe: rozwiązywanie problemów, analizowanie, wnioskowanie, wyjaśnianie, rozumowanie logiczne. Ważna jest koordynacja wzrokowo-ruchowa oraz sprawność układu mięśniowo-szkieletowego, ze względu na długotrwałą pracę przy komputerze.

Przeciwwskazaniem do pracy w zawodzie jest niesprawność intelektualna.

WAŻNE:

O stanie zdrowia i ewentualnych przeciwwskazaniach do wykonywania zawodu orzeka lekarz medycyny pracy.

Więcej informacji znajduje się w sekcji: 4.4. Możliwości zatrudnienia osób niepełnosprawnych w zawodzie.

2.5. Wykształcenie, tytuły zawodowe, kwalifikacje i uprawnienia niezbędne/preferowane do podjęcia pracy w zawodzie

Wykształcenie niezbędne do podjęcia pracy w zawodzie

Do wykonywania zawodu **specjalista do spraw systemów zarządzania bezpieczeństwem informacji** preferowane jest wykształcenie wyższe, co najmniej studia I stopnia lub studia podyplomowe z zakresu: zarządzania informacją, teleinformatyki, informacji naukowej lub pokrewnych.

Tytuły zawodowe, kwalifikacje i uprawnienia niezbędne/preferowane do podjęcia pracy w zawodzie

Podjęcie pracy w zawodzie **specjalista do spraw systemów zarządzania bezpieczeństwem informacji** ułatwia posiadanie dyplomu ukończenia studiów wyższych (studia I i II stopnia) oraz studiów podyplomowych z zakresu zarządzania informacją, teleinformatyki, informacji naukowej lub pokrewnych.

W zależności od wdrożonych w organizacji systemów zarządzania, w podjęciu pracy pomocne (lub wymagane) może być posiadanie certyfikatów:

- audytora wewnętrznego ISO⁹ 27001,
- pełnomocnika według normy ISO 27001 – Technika informatyczna – Techniki bezpieczeństwa-Systemy zarządzania bezpieczeństwem informacji,
- pełnomocnika jakości według normy ISO 9001 – System zarządzania jakością – Wymagania,

- ISO 31000, Zarządzanie ryzykiem – Wytyczne,
- pełnomocnika według normy ISO 22301 – Zarządzanie Ciągłością Działania.

Dodatkowym atutem przy zatrudnianiu może być znajomość dedykowanego oprogramowania stosowanego przez organizację.

W dużych międzynarodowych firmach specyfika pracy wymusza konieczność dobrej znajomości języka angielskiego, który zwykle jest niezbędny do sprawnego korzystania z systemów informatycznych i innych źródeł informacji.

Więcej informacji znajduje się w sekcji: 4.2. Instytucje oferujące kształcenie, szkolenie i/lub potwierdzanie kompetencji w ramach zawodu.

2.6. Możliwości rozwoju zawodowego, awansu i potwierdzania kompetencji

Możliwości rozwoju zawodowego i awansu

W zawodzie **specjalista do spraw systemów zarządzania bezpieczeństwem informacji** nie występuje uregulowana ścieżka awansu. Osoby pracujące w tym zawodzie często zaczynają karierę zawodową jako pasjonaci zagadnień informatycznych, ekonomicznych lub członkowie zespołów współtworzących obieg dokumentów, procedur wewnętrznych wdrażanych w organizacji.

Posiadając kilkuletnie doświadczenie można awansować na stanowisko kierownicze w obszarze, w którym pracownik wykonywał wcześniej swoje obowiązki.

Specjalista do spraw systemów zarządzania bezpieczeństwem informacji po nabyciu doświadczenia, uzupełnieniu wiedzy oraz złożeniu egzaminu na audytora wewnętrznego systemu bezpieczeństwa informacji według danej normy ISO, może pełnić w organizacji funkcję certyfikowanego pełnomocnika jakości lub audytora bezpieczeństwa.

Możliwość dalszego rozwoju zawodowego można uzyskać poprzez:

- kształcenie na studiach II i III stopnia,
- rozszerzenie swoich kompetencji zawodowych poprzez podejmowanie kształcenia i/lub szkolenia w zawodach pokrewnych.

Możliwości potwierdzania kompetencji

Obecnie (2018 r.) w zawodzie **specjalista do spraw systemów zarządzania bezpieczeństwem informacji** nie ma możliwości potwierdzania kompetencji zawodowych w systemie edukacji formalnej.

Alternatywną drogę potwierdzania kompetencji w tym zawodzie stanowi edukacja pozaformalna (kursy, szkolenia). Certyfikaty potwierdzające kompetencje zdobywane w ten sposób (np. audytora wewnętrznego systemu bezpieczeństwa informacji) wydawane są przez stowarzyszenia branżowe, instytucje szkoleniowe i jednostki certyfikujące.

Więcej informacji można uzyskać w Bazie Usług Rozwojowych <https://uslugirozwojowe.parp.gov.pl> oraz Zintegrowanym Rejestrze Kwalifikacji <https://rejestr.kwalifikacje.gov.pl>

2.7. Zawody pokrewne

Osoba zatrudniona w zawodzie **specjalista do spraw systemów zarządzania bezpieczeństwem informacji** może rozszerzać swoje kompetencje zawodowe w zawodach pokrewnych:

Nazwa zawodu pokrewnego zgodnie z Klasyfikacją zawodów i specjalności	Kod zawodu
Administrator bezpieczeństwa informacji (Inspektor ochrony danych)	242111
Konsultant do spraw systemów teleinformatycznych	251102
Projektant/architekt systemów teleinformatycznych	251103
Specjalista bezpieczeństwa oprogramowania	252901
Specjalista bezpieczeństwa systemów teleinformatycznych	252902
Specjalista informacji naukowej, technicznej i ekonomicznej	262206
Specjalista zarządzania informacją	262207
Specjalista zarządzania dokumentacją	262208

3. ZADANIA ZAWODOWE I WYMAGANE KOMPETENCJE

3.1. Zadania zawodowe

Pracownik w zawodzie **specjalista do spraw systemów zarządzania bezpieczeństwem informacji** wykonuje różnorodne zadania, do których należą w szczególności:

- Z1 Opracowywanie i gromadzenie dokumentacji systemu zarządzania bezpieczeństwem informacji.
- Z2 Przechowywanie i nadzorowanie zbiorów informacji, selekcjonowanie informacji.
- Z3 Obsługiwanie dedykowanych systemów informatycznych związanych z zapewnieniem bezpieczeństwa informacji.
- Z4 Zarządzanie bezpieczeństwem informacji w procesach biznesowych organizacji.
- Z5 Nadzorowanie, monitorowanie i kontrolowanie zakresu bezpieczeństwa informacji.
- Z6 Zarządzanie ryzykiem bezpieczeństwa informacji oraz ciągłością świadczonych usług.
- Z7 Opracowywanie i wdrażanie zmian w procedurach bezpieczeństwa oraz systemach informatycznych.
- Z8 Prowadzenie szkoleń pracowników organizacji z systemu zarządzania bezpieczeństwem informacji.
- Z9 Testowanie oraz odtwarzanie działań naprawczych w systemie bezpieczeństwa.
- Z10 Nadzorowanie partnerów współtworzących system zarządzania bezpieczeństwem informacji.

3.2. Kompetencja zawodowa Kz1: Pozyskiwanie, weryfikowanie i przechowywanie informacji

Kompetencja zawodowa Kz1: Pozyskiwanie, weryfikowanie i przechowywanie informacji obejmuje zestaw zadań zawodowych Z1, Z2, Z3, do realizacji których wymagane są odpowiednie zbiory wiedzy i umiejętności.

Z1 Opracowywanie i gromadzenie i dokumentacji systemu zarządzania bezpieczeństwem informacji	
WIEDZA – zna i rozumie:	UMIEJĘTNOŚCI – potrafi:
- Procesy związane z zarządzaniem informacją występujące w organizacji; - Technologie informacyjne w zakresie pozyskania, gromadzenia i utrzymania informacji;	- Identyfikować procesy związane z zarządzaniem informacją występujące w organizacji; - Wykorzystywać technologie informacyjne do pozyskania, gromadzenia i utrzymania informacji;

• Przepisy prawne dotyczące gromadzenia i utrzymania informacji; • Działanie systemów informatycznych do gromadzenia informacji.	• Stosować przepisy prawne do gromadzenia i utrzymania informacji; • Korzystać z systemów informatycznych rejestrujących informacje.
---	---

Z2 Przechowywanie i nadzorowanie zbiorów informacji, selekcjonowanie informacji

WIEDZA – zna i rozumie:	UMIEJĘTNOŚCI – potrafi:
• Przepisy prawa dotyczące przechowywania i nadzorowania informacji; • Działanie <u>hurtowni danych</u>⁶ do zarządzania systemami informacyjnymi; • Metody przechowywania i nadzorowania informacji; • Techniki konstruowania zapytań do <u>repozytoriów informacyjnych</u>²⁰; • Języki programowania; • Zasady selekcjonowania informacji wewnętrznej i zewnętrznej; • Normy, standardy i techniki Międzynarodowego i Polskiego Komitetu Normalizacyjnego.	• Analizować i stosować przepisy prawa dotyczące przechowywania i nadzorowania informacji; • Korzystać z hurtowni danych do zarządzania systemami informacyjnymi; • Przechowywać i nadzorować informację według założonych metod; • Przygotowywać zapytania do repozytoriów informacyjnych (systemów informacyjnych); • Określać zasady selekcjonowania informacji; • Interpretować normy, standardy i techniki zarządzania bezpieczeństwem informacji.

Z3 Obsługiwanie dedykowanych systemów informatycznych związanych z zapewnieniem bezpieczeństwa informacji

WIEDZA – zna i rozumie:	UMIEJĘTNOŚCI – potrafi:
• Działanie programów do gromadzenia informacji; • Obsługę klienta poczty elektronicznej; • <u>Topologie sieci komputerowej</u>²⁵ i ich <u>protokoły internetowe</u>¹⁹; • Działania programów antywirusowych i antyspamowych; • Zasady elektronicznego archiwizowania danych; • Zasady działania systemów alarmowych i wczesnego ostrzegania; • Zasady działania systemów komputerowych wspomagających procesy produkcyjne.	• Obsługiwać programy do gromadzenia informacji; • Obsługiwać różne rodzaje poczty elektronicznej; • Rozróżniać topologię sieci komputerowej i protokoły internetowe; • Korzystać z programów antywirusowych i antyspamowych; • Wyszukiwać i przetwarzać zarchiwizowane dane; • Nadzorować działanie systemów alarmowych i wczesnego ostrzegania; • Czytać i analizować działania systemów komputerowych wspomagających procesy produkcyjne.

3.3. Kompetencja zawodowa Kz2: Zarządzanie systemem bezpieczeństwa informacji

Kompetencja zawodowa Kz2: Zarządzanie systemem bezpieczeństwa informacji obejmuje zestaw zadań zawodowych Z4, Z5, Z6, do realizacji których wymagane są odpowiednie zbiory wiedzy i umiejętności.

Z4 Zarządzanie bezpieczeństwem informacji w procesach biznesowych organizacji	
WIEDZA – zna i rozumie:	UMIEJĘTNOŚCI – potrafi:
• Technologie informacyjne w zakresie bezpieczeństwa informacji; • Zasady funkcjonowania zabezpieczeń informatycznych; • Narzędzia i techniki kontroli zabezpieczenia zbiorów informacji; • Zasady współpracy z użytkownikami systemu bezpieczeństwa informacji.	• Stosować odpowiednie technologie w zakresie bezpieczeństwa informacji; • Diagnostować funkcjonowanie zabezpieczeń informatycznych; • Stosować narzędzia i techniki kontroli zabezpieczenia zbiorów informacji; • Współpracować z użytkownikami systemu bezpieczeństwa informacji.
Z5 Nadzorowanie, monitorowanie i kontrolowanie zakresu bezpieczeństwa informacji	
WIEDZA – zna i rozumie:	UMIEJĘTNOŚCI – potrafi:
• Rodzaje parametrów poddawanych analizie w procesie zabezpieczania informacji; • Kategoryzowanie zdarzeń bezpieczeństwa informacji; • Formaty, standardy rejestracji dokumentów związanych z bezpieczeństwem informacji; • Rodzaje zabezpieczeń informacji; • Procedury wewnętrzne związane z przygotowaniem dokumentacji bezpieczeństwa; • Technologie informatyczne stosowane w przetwarzaniu i <u>kategoryzowaniu informacji</u>¹¹. • Planowanie i wykonywanie zadań uczestników zabezpieczających zbiory danych; • Wartość poszczególnych składników kosztowych procesu bezpieczeństwa informacji; • Konsekwencje kar i działań naprawczych <u>jednostek kontrolnych</u>¹⁰.	• Analizować parametry przetworzonych informacji; • Stosować właściwy rodzaj zabezpieczeń informacji zastosowany w organizacji; • Przygotowywać dokumenty związane z bezpieczeństwem informacji w poszczególnych komórkach organizacyjnych; • Stosować dokumentację wynikającą z procedur wewnętrznych związanych z bezpieczeństwem; • Korzystać z narzędzi informatycznych stosowanych w przetwarzaniu i kategoryzowaniu informacji; • Zarządzać wykonywaniem zadań uczestników zabezpieczających zbiory danych; • Określać i szacować poszczególne składniki kosztowe procesu bezpieczeństwa informacji; • Wyciągać wnioski z nałożonych kar i rekomendować działania naprawcze.
Z6 Zarządzanie ryzykiem bezpieczeństwa informacji oraz ciągłości świadczonych usług	
WIEDZA – zna i rozumie:	UMIEJĘTNOŚCI – potrafi:
• Wytyczne organizacji w zakresie zarządzania ryzykiem bezpieczeństwa informacji i ciągłości działania; • Modele szacowania i zarządzania ryzykiem bezpieczeństwa informacji; • Przykłady niepożądanych zdarzeń w obszarze zasobów ludzkich, infrastruktury, środowiska pracy i ich podatność na zagrożenia w systemie	• Zarządzać ryzykiem bezpieczeństwa informacji i ciągłości działania; • Zarządzać ryzykiem bezpieczeństwa i stosować modele <u>szacowania ryzyka</u>²³ bezpieczeństwa informacji; • Przewidywać konsekwencje niepożądanego zdarzenia; • Szacować prawdopodobieństwo i skutek

bezpieczeństwa informacji.	wystąpienia zagrożeń systemu bezpieczeństwa informacji.
----------------------------	---

3.4. Kompetencja zawodowa Kz3: Wdrażanie, nadzorowanie i aktualizowanie systemu zarządzania bezpieczeństwem informacji

Kompetencja zawodowa Kz3: Wdrażanie, nadzorowanie i aktualizowanie systemu zarządzania bezpieczeństwem informacji obejmuje zestaw zadań zawodowych Z7, Z8, Z9, Z10, do realizacji których wymagane są odpowiednie zbiory wiedzy i umiejętności.

Z7 Opracowywanie i wdrażanie zmian w procedurach bezpieczeństwa oraz systemach informatycznych	
WIEDZA – zna i rozumie:	UMIEJĘTNOŚCI – potrafi:
- Rozwiązania i techniki wdrażania procedur bezpieczeństwa; - Działania oraz procedury bezpieczeństwa poszczególnych <u>właścicieli procesów</u>²⁶; - Zasady <u>nadzoru nad dokumentami i zapisami</u>¹³ bezpieczeństwa informacji; - Zasady tworzenia dokumentacji systemów zabezpieczających tajemnice państwowe i służbowe, przepisy o ochronie danych osobowych, higieny pracy, ochrony przeciwpożarowej i ochrony środowiska.	- Adaptować do potrzeb organizacji dostępne rozwiązania i zmiany w procedurach bezpieczeństwa; - Łączyć podstawowe działania w organizacji z procedurami bezpieczeństwa u poszczególnych właścicieli procesów; - Przygotowywać i wdrażać nadzór nad dokumentami i zapisami bezpieczeństwa informacji; - Zachowywać zgodność z różnymi systemami zabezpieczającymi tajemnice państwowe i służbowe, przepisami o ochronie danych osobowych, higieny pracy, ochronie przeciwpożarowej, ochronie środowiska i integrować je w jeden system jakości.

Z8 Prowadzenie szkoleń pracowników organizacji z systemu zarządzania bezpieczeństwem informacji	
WIEDZA – zna i rozumie:	UMIEJĘTNOŚCI – potrafi:
- Zasady polityki bezpieczeństwa organizacji w zakresie wykonywania obowiązków zawodowych; - Zasady współpracy z użytkownikami i motywowania ich do chronienia przetwarzanej informacji; - Potrzeby szkoleniowe w ramach przyjętych celów ścisłego kierownictwa; - Zasady prezentowania i prowadzenia szkoleń z systemu zarządzania bezpieczeństwem informacji.	- Wdrażać i przekazywać pracownikom zasady polityki bezpieczeństwa organizacji w zakresie wykonywania obowiązków zawodowych; - Motywować do współpracy użytkowników w zakresie przetwarzania i przechowywania informacji oraz danych osobowych; - Analizować potrzeby szkoleniowe zgodnie z przyjętym systemem zarządzania bezpieczeństwem informacji; - Prezentować i prowadzić szkolenia z systemu zarządzania bezpieczeństwem informacji.

Z9 Testowanie oraz odtwarzanie działań naprawczych w systemie bezpieczeństwa	
WIEDZA – zna i rozumie:	UMIEJĘTNOŚCI – potrafi:
Zagadnienia związane z analizą obciążenia serwerów, stacji roboczych i optymalizacji ich wykorzystania;	- Analizować obciążenia i wydajność serwerów oraz wdrażać działania naprawcze; - Diagnostować prawidłowość działania sieci

• Zasady działania sieci informatycznych, <u>dzienników zdarzeń/logów</u>⁵ oraz wykresów pomocniczych z aplikacji serwerowych; • Zasady działań naprawczych lub korygujących w systemie bezpieczeństwa.	informatycznych na podstawie dzienników zdarzeń/logów oraz wykresów pomocniczych z aplikacji serwerowych; • Wyciągać wnioski z zaistniałych działań naprawczych lub korygujących w systemie bezpieczeństwa.
---	--

Z10 Nadzorowanie partnerów współtworzących system zarządzania bezpieczeństwem informacji	
WIEDZA – zna i rozumie:	UMIEJĘTNOŚCI – potrafi:
• Zasady zarządzania bezpieczeństwem informacji panujące w branży; • Techniki audytów przeprowadzanych w różnych branżach; • Raporty i sprawozdania branżowe; • Zasady nadzoru nad dokumentami i zapisami procedur raportowania.	• Stosować branżowe zasady bezpieczeństwa informacji; • Stosować techniki audytów w zależności od audytowanego procesu; • Przygotowywać raporty i sprawozdania branżowe; • Nadzorować dokumenty i zapisy procedur raportowania.

3.5. Kompetencje społeczne

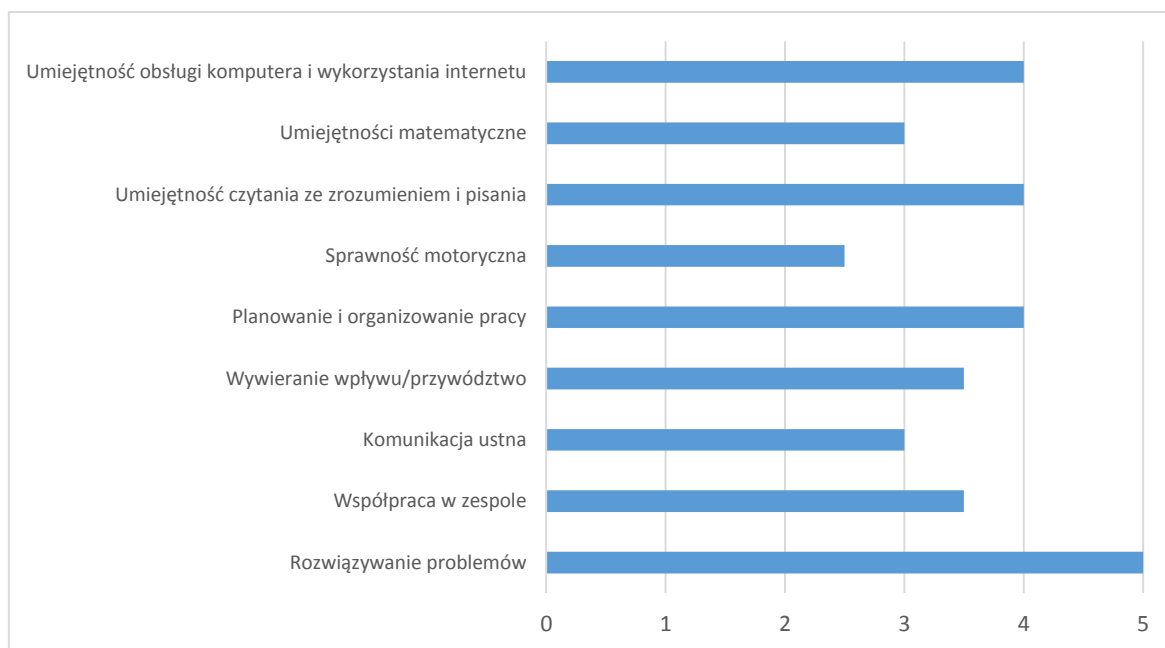
Pracownik w zawodzie **specjalista do spraw systemów zarządzania bezpieczeństwem informacji** powinien posiadać kompetencje społeczne niezbędne do prawidłowego i skutecznego wykonywania zadań zawodowych.

W szczególności pracownik jest gotów do:

- Ponoszenia odpowiedzialności za obsługiwane systemy informatyczne i źródła informacji wykorzystywane w tych systemach.
- Ponoszenia odpowiedzialności za skutki podejmowanych decyzji i działań w zakresie zarządzania bezpieczeństwem informacji.
- Kierowania się zasadami etyki zawodowej, w tym przestrzegania zasad uczciwości, rzetelności, poufności.
- Podejmowania inicjatyw zmierzających do skutecznego nadzoru nad systemem informatycznym i doskonalenia jego działania.
- Komunikowania się ze stronami zarządzającymi systemem bezpieczeństwa.
- Doskonalenia własnych kompetencji zawodowych w dziedzinie zarządzania bezpieczeństwem informacji.

3.6. Profil kompetencji kluczowych dla zawodu

Pracownik powinien mieć zdolność właściwego wykonywania zadań zawodowych i predyspozycje do rozwoju zawodowego. Dlatego wymaga się od niego odpowiednich kompetencji kluczowych. Zostały one zilustrowane w formie profilu (rys. 1) ukazującego wagę kompetencji kluczowych dla zawodu **specjalista do spraw systemów zarządzania bezpieczeństwem informacji**.



Rys. 1. Profil kompetencji kluczowych dla zawodu **specjalista do spraw systemów zarządzania bezpieczeństwem informacji**

Uwaga:

Wykaz kompetencji kluczowych opracowano na podstawie wykazu stosowanego w Międzynarodowym Badaniu Kompetencji Osób Dorosłych – projekt PIAAC (OECD).

3.7. Powiązanie kompetencji zawodowych z opisami poziomów Polskiej Ramy Kwalifikacji oraz Sektorowej Ramy Kwalifikacji

Kompetencje zawodowe pracownika w zawodzie **specjalista do spraw systemów zarządzania bezpieczeństwem informacji** nawiązują do opisów poziomów Polskiej Ramy Kwalifikacji.

Opis zawodu, zadań zawodowych i wymagań kompetencyjnych może stanowić materiał informacyjny dla przygotowania (lub aktualizacji) opisów kwalifikacji wprowadzanych do Zintegrowanego Systemu Kwalifikacji (ZSK). Więcej informacji:

- Zintegrowany System Kwalifikacji: <https://www.kwalifikacje.gov.pl>
- Zintegrowany Rejestr Kwalifikacji: <https://rejestr.kwalifikacje.gov.pl>

4. ODNIESIENIE DO SYTUACJI ZAWODU NA RYNKU PRACY I MOŻLIWOŚCI DOSKONALENIA ZAWODOWEGO

4.1. Możliwości podjęcia pracy w zawodzie

Specjalista do spraw systemów zarządzania bezpieczeństwem informacji może ubiegać się o pracę w organizacji, w której informacja jest tworzona, przechowywana, niszczona, przetwarzana, przekazywana, wykorzystywana, utracona lub uszkodzona. Podmioty, w których może znaleźć zatrudnienie to, np.:

- przedsiębiorstwa produkcyjne i usługowe dowolnej branży, w szczególności sektora bankowego, informatycznego, energetycznego, ochrony zdrowia,
- instytucje rządowe i samorządowe,
- jednostki badawcze, rozwojowe, naukowe,
- archiwa – publiczne, w tym państwowe oraz prywatne.

Funkcja specjalisty do spraw systemów zarządzania bezpieczeństwem informacji może być łączona z innymi zawodami informatycznymi.

Wykonując ten zawód można być pracownikiem etatowym lub pracować na zlecenie.

Specjalista może założyć własną działalność gospodarczą i świadczyć usługi dla wielu organizacji (np. jako certyfikowany audytor systemów zarządzania bezpieczeństwem informacji).

WAŻNE:

Zachęcamy do sprawdzenia dostępnych ofert pracy w **Centralnej Bazie Ofert Pracy:**

<http://oferty.praca.gov.pl>

Natomiast aktualizacje informacji o możliwościach zatrudnienia w zawodzie, przyszłe zapotrzebowanie na dany zawód na rynku pracy oraz dodatkowe informacje można uzyskać, korzystając z **polecanych źródeł danych**.

Polecane źródła danych [dostęp: 31.10.2018]:

Ranking (monitoring) zawodów deficytowych i nadwyżkowych:

<http://mz.praca.gov.pl>

<https://www.gov.pl/web/rodzina/zawody-deficytowe-zrownowazone-i-nadwyzkowe>

Barometr zawodów: <https://barometrzawodow.pl>

Wojewódzkie obserwatoria rynku pracy:

Mazowieckie – <http://obserwatorium.mazowsze.pl>

Małopolskie – <https://www.obserwatorium.malopolska.pl>

Lubelskie – <http://lorp.wup.lublin.pl>

Regionalne Obserwatorium Rynku Pracy w Łodzi – <http://obserwatorium.wup.lodz.pl>

Pomorskie – <http://www.porp.pl>

Opolskie – <http://www.obserwatorium.opole.pl>

Wielkopolskie – <http://www.obserwatorium.wup.poznan.pl>

Zachodniopomorskie – <https://www.wup.pl/pl/dla-instytucji/zachodniopomorskie-obserwatorium-ryнку-pracy>

Podlaskie – <http://www.obserwatorium.up.podlasie.pl>

Zielona Linia. Centrum Informacyjne Służb Zatrudnienia:

<http://zielonalinia.gov.pl>

Portal Prognozowanie Zatrudnienia:

www.prognozowaniezatrudnienia.pl

Portal EU Skills Panorama:

<http://skillspanorama.cedefop.europa.eu/en>

Europejski portal mobilności zawodowej EURES:

<https://eures.praca.gov.pl>

<https://ec.europa.eu/eures/public/pl/homepage>

4.2. Instytucje oferujące kształcenie, szkolenie i/lub potwierdzanie kompetencji w ramach zawodu

Kształcenie

Obecnie (2018 r.) do pracy w zawodzie **specjalista do spraw systemów zarządzania bezpieczeństwem informacji** przygotowują w Polsce liczne szkoły wyższe na studiach I i II oraz III stopnia na kierunkach z obszaru zarządzania informacją, teleinformatyki, informacji naukowej. Kierunki te posiadają w swej ofercie zarówno uczelnie techniczne, jak i uniwersytety.

Wiele uczelni w Polsce oferuje także kształcenie w systemie studiów podyplomowych dla absolwentów szkół wyższych, pragnących poszerzyć swoją wiedzę z zakresu wybranych zagadnień związanych z bezpieczeństwem systemów teleinformatycznych.

Szkolenie

Na rynku dostępna jest szeroka oferta instytucji szkoleniowych, stowarzyszeń branżowych, uczelni organizujących szkolenia dla osób pracujących w zawodzie **specjalista do spraw systemów zarządzania bezpieczeństwem informacji**. Z ich oferty korzystają często pracodawcy, organizując wewnętrzne szkolenia dla swoich pracowników.

Dodatkowe szkolenia proponują producenci systemów informatycznych, systemów obiegu informacji i urzędów zabezpieczających, oferując sprzedaż i prezentację własnych produktów.

Przykładowa tematyka szkoleń:

- bezpieczeństwo informacji,
- zarządzanie ciągłością działania,
- zarządzanie ryzykiem,
- norma ISO/IEC 27001 (zarządzanie bezpieczeństwem informacji) – wymagania i wdrożenie,
- norma ISO/IEC 27001 (zarządzanie bezpieczeństwem informacji) – szacowanie i postępowanie z ryzykiem.

WAŻNE:

Więcej informacji o instytucjach oferujących kształcenie, szkolenie i/lub walidację kompetencji w ramach zawodu można uzyskać, korzystając z **polecanych źródeł danych**.

Polecane źródła danych [dostęp: 31.10.2018]:

Szkolnictwo wyższe:

www.wyberzstudia.nauka.gov.pl

Szkolnictwo zawodowe:

<https://www.ore.edu.pl/category/ksztalcenie-zawodowe-i-ustawiczne>

<http://doradztwo.ore.edu.pl/wyberam-zawod>

<https://zrp.pl>

Szkolenia zawodowe:

Rejestr Instytucji Szkoleniowych – <http://www.stor.praca.gov.pl/portal/#/ris>

Baza Usług Rozwojowych – <https://uslugirozwojowe.parp.gov.pl>

Inne źródła danych:

Zintegrowany Rejestr Kwalifikacji – <https://rejestr.kwalifikacje.gov.pl>

Bilans Kapitału Ludzkiego – <https://bkl.parp.gov.pl>

Fundacja Rozwoju Systemu Edukacji – <http://www.frse.org.pl>, <http://europass.org.pl>

Learning Opportunities and Qualifications in Europe – <https://ec.europa.eu/ploteus>

4.3. Zarobki osób wykonujących dany zawód/daną grupę zawodów

Wynagrodzenie (2018 r.) osób pracujących w zawodzie **specjalista do spraw systemów zarządzania bezpieczeństwem informacji** jest zróżnicowane i wynosi najczęściej od 3500 zł do 8000 zł brutto miesięcznie w przeliczeniu na jeden etat, a w szczególności np.:

- 3500 zł do 5000 zł brutto dla osób wykonujących pracę specjalisty do spraw bezpieczeństwa informatycznego,
- 4000 zł do 8000 zł brutto na stanowiskach wymagających dodatkowych umiejętności lub przeszkolenia, np. w zakresie certyfikowanego pełnomocnika systemów bezpieczeństwa informacji, audytora wewnętrznego, administratora bezpieczeństwa informacji, ochrony danych osobowych.

Wysokość wynagrodzenia uzależniona jest od wielkości organizacji, obszarów objętych systemem bezpieczeństwa oraz skalą dokumentacji wymaganej do zarządzania informacją.

Zarobki osób prowadzących własną działalność gospodarczą, np. jako certyfikowani audytorzy systemów zarządzania bezpieczeństwem informacji, uzależnione są od liczby pozyskanych i zrealizowanych zleceń.

WAŻNE:

Zarobki osób wykonujących dany zawód/grupę zawodów są orientacyjne i mogą szybko stracić aktualność. Dlatego na bieżąco należy sprawdzać, jakie zarobki oferuje rynek pracy, korzystając z **polecanych źródeł danych**.

Polecane źródła danych [dostęp: 31.10.2018]:

Wynagrodzenie w Polsce według danych GUS:

<http://stat.gov.pl/obszary-tematyczne/rynek-pracy/pracujacy-zatrudnieni-wynagrodzenia-koszty-pracy>

Przykładowe portale informujące o zarobkach:

<https://wynagrodzenia.pl/gus>

<https://wynagrodzenia.pl/kategoria/zarobki-na-stanowiskach-i-szczegolach>

<https://sedlak.pl/raporty-placowe>

<https://zarobki.pracuj.pl>

<https://www.forbes.pl/ogolnopolskie-badanie-wynagrodzen>

<https://www.kariera.pl/wynagrodzenia>

4.4. Możliwości zatrudnienia osób niepełnosprawnych w zawodzie

W zawodzie **specjalista do spraw systemów zarządzania bezpieczeństwem informacji** możliwe jest zatrudnienie osób niepełnosprawnych.

Warunkiem niezbędnym jest identyfikacja indywidualnych barier i dostosowanie technicznych i organizacyjnych warunków środowiska oraz stanowiska pracy do potrzeb zatrudnienia osób:

- z niewielką dysfunkcją kończyn górnych (05-R), która nie wyklucza pracy przy komputerze,
- z niewielką dysfunkcją kończyn dolnych (05-R), która nie wyklucza możliwości swobodnego przemieszczania się,
- z wadami i dysfunkcją wzroku (04-O), w przypadku możliwości skorygowania ich szklami optycznymi lub soczewkami kontaktowymi,
- z dysfunkcją narządu słuchu (03-L), pod warunkiem, że niepełnosprawność ta jest możliwa do skorygowania za pomocą aparatów słuchowych,
- z epilepsją (06-E) na wybranych stanowiskach pracy, pod warunkiem, że napady padaczkowe występują sporadycznie,
- z innymi rodzajami niepełnosprawności wynikającymi z chorób układu krążenia, oddechowego, pokarmowego, moczowo-płciowego i innymi, pod warunkiem, że praca nie wymaga znacznego wysiłku fizycznego lub jest zorganizowana w taki sposób, aby pracownik miał możliwość regularnego przyjmowania leków.

WAŻNE:

Decyzja o zatrudnieniu osoby z jakimkolwiek rodzajem niepełnosprawności może być podjęta wyłącznie po indywidualnej konsultacji z lekarzem medycyny pracy.

5. ODNIESIENIE DO EUROPEJSKIEJ KLASYFIKACJI UMIEJĘTNOŚCI/KOMPETENCJI, KWALIFIKACJI I ZAWODÓW (ESCO)

Europejska klasyfikacja umiejętności/kompetencji, kwalifikacji i zawodów (European Skills/Competences, Qualifications and Occupations – ESCO) jest narzędziem łączącym rynek edukacji z rynkiem pracy. ESCO jest częścią strategii „Europa 2020”. W klasyfikacji określono i uszeregowano umiejętności, kompetencje, kwalifikacje i zawody istotne dla unijnego rynku pracy oraz kształcenia i szkolenia. Tworzenie europejskiego rynku pracy, a w przyszłości wspólnego obszaru kształcenia ustawicznego wymaga, aby zdobywane przez jednostki umiejętności oraz kwalifikacje były zrozumiałe oraz łatwo porównywalne między krajami, a także – by promowały mobilność wśród pracowników.

Obecnie (2018 r.) klasyfikacja ESCO jest dostępna w 27 językach (w 24 językach UE, islandzkim, norweskim i arabskim) za pośrednictwem platformy ESCO: <https://ec.europa.eu/esco/portal/home>

Klasyfikacja ESCO została oparta na trzech filarach i pokazuje w sposób systematyczny relacje między nimi:

- **Zawody:** <https://ec.europa.eu/esco/portal/occupation>
- **Umiejętności/Kompetencje:** <https://ec.europa.eu/esco/portal/skill>
- **Kwalifikacje:** <https://ec.europa.eu/esco/portal/qualification>

6. ŹRÓDŁA DODATKOWYCH INFORMACJI O ZAWODZIE

Podstawowe regulacje prawne:

Stan prawny na dzień: 31.10.2018 r.

- Ustawa z dnia 20 lipca 2018 r. - Prawo o szkolnictwie wyższym i nauce (Dz. U. poz. 1668, z późn. zm.).
- Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. poz. 1560).
- Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. poz. 1000, z późn. zm.).
- Ustawa z dnia 22 grudnia 2015 r. o Zintegrowanym Systemie Kwalifikacji (t.j. Dz. U. z 2017 r. poz. 986, z późn. zm.).
- Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (t.j. Dz. U. z 2018 r. poz. 412, z późn. zm.).
- Ustawa z dnia 20 kwietnia 2004 r. o promocji zatrudnienia i instytucjach rynku pracy (t.j. Dz. U. z 2018 r. poz. 1265, z późn. zm.).
- Ustawa z dnia 6 września 2001 r. o dostępie do informacji publicznej (t.j. Dz. U. z 2018 r. poz. 1330, z późn. zm.).
- Ustawa z dnia 27 lipca 2001 r. o ochronie baz danych (Dz. U. Nr 128, poz. 1402, z późn. zm.).
- Ustawa z dnia 27 czerwca 1997 r. o bibliotekach (t.j. Dz. U. z 2018 r. poz. 574, z późn. zm.).
- Ustawa z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (t.j. Dz. U. z 2018 r. poz. 1191, z późn. zm.).
- Rozporządzenie Ministra Edukacji Narodowej z dnia 13 kwietnia 2016 r. w sprawie charakterystyk drugiego stopnia Polskiej Ramy Kwalifikacji typowych dla kwalifikacji o charakterze zawodowym - poziomy 1–8 (Dz. U. poz. 537).
- Rozporządzenie Ministra Pracy i Polityki Społecznej z dnia 7 sierpnia 2014 r. w sprawie klasyfikacji zawodów i specjalności na potrzeby rynku pracy oraz zakresu jej stosowania (t.j. Dz. U. z 2018 r. poz. 227).
- Norma PN-EN ISO 9001, System zarządzania jakością – Wymagania.
- Norma PN-EN ISO/IEC 27001, Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji.
- Norma PN-EN ISO/IEC 27002, Technika informatyczna – Techniki bezpieczeństwa – Praktyczne zasady zarządzania bezpieczeństwem informacji.
- Norma PN-ISO 31000, Zarządzanie ryzykiem – Wytyczne.

Literatura branżowa:

- Białas A.: Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie. PWN, Warszawa 2017.
- Control Engineering Polska – czasopismo branżowe. Wydawnictwo Trade Media International Sp. z o.o., Warszawa.
- Czupryński A.: Nauki o bezpieczeństwie. Wybrane problemy badań. Wydawnictwo CNBOP-PIB, Józefów 2018.
- ITIL Foundation Handbook – Pocketbook from the Official Publisher of ITIL. TSO, 2012.
- Liderman K.: Bezpieczeństwo informacyjne. PWN, Warszawa 2012.

- Owczarek K., Żurak-Owczarek, C.: Systemy informatyczne w zarządzaniu łańcuchem dostaw. Logistyka, nr 4/2015.
- Pacana A., Stadnicka D.: Wdrażanie i auditowanie systemów zarządzania jakością zgodnych z normą ISO 9001:2000. Oficyna Wydawnicza Politechniki Rzeszowskiej, Rzeszów 2007.
- Polaczek T.: Audyt bezpieczeństwa informacji w praktyce. Helion, Gliwice 2006.
- Problemy jakości – czasopismo branżowe. Czasopismo Federacji Stowarzyszeń Naukowo-Technicznych NOT, Warszawa.
- Sienkiewicz P. (red.): Inżynieria systemów bezpieczeństwa. PWE, Warszawa 2015.
- Skomra W. (red.): Metodyka oceny ryzyka na potrzeby systemu zarządzania kryzysowego RP. Szkoła Główna Służby Pożarniczej, Warszawa 2015.
- Solecki A., Solecki P.: Zarządzanie bezpieczeństwem informacji i programami antykorupcyjnymi. Wyższa Szkoła Administracji, Bielsko-Biała 2007.
- Tabakow M., Korczak J., Franczyk B.: Big data – definicje, wyzwania i technologie informatyczne. Informatyka Ekonomiczna, Wrocław 2014.
- Trocki M.: Outsourcing: metoda restrukturyzacji działalności gospodarczej. PWE, Warszawa 2001.
- Wróbel P.: Problemy zarządzania telepracownikami. Prace i materiały Wydziału Zarządzania Uniwersytetu Gdańskiego, nr 2/2007.
- Wróblewski D.: Zarządzanie ryzykiem. Przegląd wybranych metodyk. Wydanie rozszerzone. Wydawnictwo CNBOP-PIB, Józefów 2018.

Zasoby internetowe [dostęp: 31.10.2018]:

- Baza danych standardów kwalifikacji/kompetencji zawodowych i modułowych programów szkoleń: <ftp://kwalifikacje.praca.gov.pl>
- Międzynarodowa Organizacja Normalizacyjna: <https://www.iso.org>
- Polski Komitet Normalizacyjny: <https://www.pkn.pl>
- Polskie Towarzystwo Informatyczne: <http://www.pti.org.pl>
- Portal Asystent BHP: <https://asystentbhp.pl>
- Sektorowa Rama Kwalifikacji dla Sektora Informatycznego (SRK IT): <http://kwalifikacje.edu.pl/sektorowa-rama-kwalifikacji-dla-sektora-informatycznego>
- Standardy orzecznictwa lekarskiego ZUS: <http://www.zus.pl/lekarze/publikacje/standardy-orzecznictwa-lekarskiego-zus>
- Urząd Ochrony Danych Osobowych: <https://uodo.gov.pl>
- Wyszukiwarka opisów zawodów: <http://psz.praca.gov.pl/rynek-pracy/bazy-danych/klasyfikacja-zawodow-i-specjalnosci/wyszukiwarka-opisow-zawodow>

7. SŁOWNIK POJĘĆ

7.1. Definicje powiązane z opisem informacji o zawodzie (zawodoznawcze)

Nazwa pojęcia	Definicja pojęcia
Awans zawodowy	Wyróżnia się dwa podstawowe rodzaje awansu – pionowy oraz poziomy. Awans pionowy oznacza zmianę stanowiska na wyższe w hierarchii przedsiębiorstwa/organizacji oraz przyznanie wyższego wynagrodzenia i poszerzenie uprawnień, np. awans polegający na osiągnięciu wyższego stopnia wymagań formalnych w policji, w wojsku, mianowanie na wyższy stopień – awans nauczycielski. Awans poziomy oznacza zmianę stanowiska niepociągającą za sobą zmiany pozycji pracownika w hierarchii firmy, np. objęcie dodatkowego stanowiska przez pracownika, powierzenie nowych zadań, rozszerzenie uprawnień i zakresu podejmowanych decyzji.
Czynności zawodowe	Są to działania podejmowane w ramach zadania zawodowego i dające efekt w postaci realizacji celu przewidzianego w zadaniu zawodowym.

INFORMACJA O ZAWODZIE – Specjalista do spraw systemów zarządzania bezpieczeństwem informacji 252903

Edukacja formalna	Kształcenie realizowane przez publiczne i niepubliczne szkoły oraz inne podmioty systemu oświaty, uczelnie oraz inne podmioty systemu szkolnictwa wyższego w ramach programów, które prowadzą do uzyskania kwalifikacji pełnych oraz kwalifikacji nadawanych po ukończeniu studiów podyplomowych (zgodnie z ustawą Prawo o szkolnictwie wyższym) albo kwalifikacje w zawodzie (zgodnie z przepisami oświatowymi).
Edukacja pozaformalna	Kształcenie i szkolenie realizowane w ramach programów, które nie prowadzą do uzyskania kwalifikacji pełnych lub kwalifikacji właściwych dla edukacji formalnej.
Efekty uczenia się	Wiedza, umiejętności oraz kompetencje społeczne nabyte w procesie uczenia się (w ramach edukacji formalnej, edukacji pozaformalnej lub poprzez uczenie się nieformalne).
Europejskie Ramy Kwalifikacji (ERK)	Przyjęta w Unii Europejskiej struktura i opis poziomów kwalifikacji umożliwiające porównanie kwalifikacji uzyskiwanych w różnych państwach. W ERK wyróżniono 8 poziomów kwalifikacji opisywanych za pomocą efektów uczenia się (wiedza, umiejętności i kompetencje). ERK stanowi układ odniesienia do krajowych ram kwalifikacji, w tym do PRK.
Kody niepełnosprawności	Są symbolami rodzaju schorzenia, które ma decydujący wpływ na to, do jakich prac osoba niepełnosprawna może być kierowana, a do jakich nie powinna ze względu na jej zdrowie i skuteczność pracy na danym stanowisku. Podstawowe kody niepełnosprawności: 01-U upośledzenie umysłowe, 02-P choroby psychiczne, 03-L zaburzenia głosu, mowy i choroby słuchu, 04-O choroby narządu wzroku, 05-R upośledzenie narządu ruchu, 06-E epilepsja, 07-S choroby układu oddechowego i krążenia, 08-T choroby układu pokarmowego, 09-M choroby układu moczowo-płciowego, 10-N choroby neurologiczne, 11-I inne, w tym schorzenia: endokrynologiczne, metaboliczne, zaburzenia enzymatyczne, choroby zakaźne i odzwierzęce, zeszpecenia, choroby układu krwiotwórczego, 12-C całościowe zaburzenia rozwojowe.
Kompetencje społeczne	Jest to rozwinięta w toku uczenia się zdolność kształtowania własnego rozwoju oraz autonomicznego i odpowiedzialnego uczestniczenia w życiu zawodowym i społecznym, z uwzględnieniem etycznego kontekstu własnego postępowania.
Kompetencje kluczowe	Są to kompetencje (połączenie wiedzy, umiejętności i kompetencji społecznych) integracji społecznej i zatrudnienia potrzebne w życiu zawodowym i pozazawodowym oraz do bycia aktywnym obywatelem. Na potrzeby opracowania informacji o zawodach wyróżniono 9 kompetencji, które zostały wybrane i pogrupowane ze zbioru 15 kompetencji kluczowych wyodrębnionych w Międzynarodowym Badaniu Kompetencji Osób Dorosłych – Projekt PIAAC prowadzonym cyklicznie przez OECD.
Kompetencja zawodowa	Jest to układ wiedzy, umiejętności i kompetencji społecznych niezbędnych do wykonywania, w ramach wydzielonego zakresu pracy w zawodzie zestawu zadań zawodowych. Posiadanie jednej lub kilku kompetencji zawodowych powinno umożliwić zatrudnienie na co najmniej jednym stanowisku pracy w zawodzie.
Kwalifikacja	Oznacza zestaw efektów uczenia się w zakresie wiedzy, umiejętności oraz kompetencji społecznych nabytych w edukacji formalnej, edukacji pozaformalnej lub poprzez uczenie się nieformalne, zgodnych z ustalonymi dla danej kwalifikacji wymaganiami, których osiągnięcie zostało sprawdzone w procesie walidacji oraz formalnie potwierdzone przez uprawniony podmiot certyfikujący. W Zintegrowanym Systemie Kwalifikacji wyodrębniono 4 rodzaje kwalifikacji: pełne, częściowe, rynkowe i uregulowane.
Polska Rama Kwalifikacji (PRK)	Opis ośmiu wyodrębnionych w Polsce poziomów kwalifikacji odpowiadających odpowiednim poziomom Europejskich Ram Kwalifikacji sformułowany za pomocą ogólnych charakterystyk efektów uczenia się dla kwalifikacji na poszczególnych poziomach ujętych w kategoriach wiedzy, umiejętności i kompetencji społecznych.
Potwierdzanie kompetencji	Jest to proces polegający na sprawdzeniu, czy kompetencje wymagane dla danej kwalifikacji zostały osiągnięte. Terminy o podobnym znaczeniu: „walidacja”, „egzaminowanie”. Proces ten prowadzi do certyfikacji – wydania przez upoważnioną instytucję „dyplomu”, „świadectwa”, „certyfikatu”.

INFORMACJA O ZAWODZIE – Specjalista do spraw systemów zarządzania bezpieczeństwem informacji 252903

Sektorowa Rama Kwalifikacji (SRK)	Opis poziomów kwalifikacji funkcjonujących w danym sektorze lub branży; poziomy Sektorowych Ram Kwalifikacji odpowiadają odpowiednim poziomom Polskiej Ramy Kwalifikacji.
Sprawności sensomotoryczne	Są to sprawności związane z funkcjonowaniem narządów zmysłów (wzroku, słuchu, smaku, powonienia, dotyku) oraz narządu ruchu (sprawność rąk, precyzja ruchów rąk, sprawność nóg, koordynacja wzrokowo-ruchowa itp.).
Stanowisko pracy	Jest to miejsce pracy w strukturze organizacyjnej, np. przedsiębiorstwa, instytucji, organizacji, w ramach którego pracownik wykonuje zadania zawodowe stale lub okresowo. Do prawidłowego wykonywania zadań na danym stanowisku pracy konieczne jest posiadanie wiedzy, umiejętności oraz kompetencji społecznych właściwych dla kompetencji zawodowych wyodrębnionych w zawodzie.
Tytuł zawodowy	Jest przyznawany osobie, która udowodniła, że posiada określony zasób wiedzy i umiejętności potrzebny do wykonywania danego zawodu. W niektórych grupach zawodowych (technicy, lekarze, rzemieślnicy) istnieją ustawowo zadekretowane nazwy i hierarchie tych tytułów, podczas gdy w innych nie ma takich systemów. Przykładowo tytuły zawodowe uzyskiwane w szkołach i placówkach oświaty to: robotnik wykwalifikowany i technik, w rzemiośle: uczeń, czeladnik, mistrz, w kulturze fizycznej: trener, instruktor, menedżer sportu.
Umiejętności	Jest to przyswojona w procesie uczenia się zdolność do wykonywania zadań i rozwiązywania problemów właściwych dla dziedziny uczenia się lub działalności zawodowej.
Uprawnienia zawodowe	Oznaczają posiadanie prawa do wykonywania czynności zawodowych (zawodu), do których dostęp jest ograniczony poprzez przepisy prawne przewidujące konieczność posiadania odpowiedniego wykształcenia, spełnienia wymagań kwalifikacyjnych lub innych dodatkowych wymagań.
Uczenie się nieformalne	Uzyskiwanie efektów uczenia się poprzez różnego rodzaju aktywność poza edukacją formalną i edukacją pozaformalną, w tym poprzez samouczenie się i doświadczenie uzyskane w pracy.
Walidacja	Oznacza sprawdzenie, czy osoba ubiegająca się o nadanie określonej kwalifikacji, niezależnie od sposobu uczenia się (edukacja formalna, pozaformalna i uczenie się nieformalne) tej osoby, osiągnęła wyodrębnioną część lub całość efektów uczenia się wymaganych dla tej kwalifikacji.
Wiedza	Jest to zbiór opisów obiektów i faktów, zasad, teorii oraz praktyk przyswojonych w procesie uczenia się, odnoszących się do dziedziny uczenia się lub działalności zawodowej.
Wykształcenie	Oznacza rezultat procesu kształcenia w zakresie ogólnym i specjalistycznym charakteryzowany na podstawie: – poziomu wykształcenia odpowiadającego poziomowi ukończonej szkoły (np. wykształcenie: podstawowe, gimnazjalne, ponadpodstawowe, ponadgimnazjalne, czeladnicze, policealne, wyższe (pierwszy, drugi i trzeci stopień), – profilu wykształcenia (ukończonej szkoły) lub dziedziny wykształcenia (kierunek lub kierunek i specjalność ukończonej szkoły wyższej lub wyższej szkoły zawodowej).
Zadanie zawodowe	Jest to logiczny wycinek lub etap pracy w ramach zawodu o wyraźnie określonym początku i końcu wykonywany na stanowisku pracy. Na zadanie zawodowe składa się układ czynności zawodowych powiązanych jednym celem, kończący się określonym wytworem, usługą lub istotną decyzją. W wyniku podziału pracy każdy zawód różni się wykonywanymi zadaniami, na które składają się czynności zawodowe.
Zawód	Jest to zbiór zadań zawodowych wyodrębnionych w wyniku społecznego podziału pracy, wykonywanych przez poszczególne osoby i wymagających odpowiednich kwalifikacji i kompetencji (wiedzy, umiejętności i kompetencji społecznych), zdobytych w wyniku kształcenia lub praktyki. Wykonywanie zawodu stanowi źródło utrzymania.
Zintegrowany System Kwalifikacji (ZSK)	Wyodrębniona część Krajowego Systemu Kwalifikacji, w której obowiązują określone w ustawie standardy opisywania kwalifikacji oraz przypisywania poziomu Polskiej Ramy Kwalifikacji do kwalifikacji, zasady włączania kwalifikacji do Zintegrowanego Systemu Kwalifikacji i ich ewidencjonowania w Zintegrowanym Rejestrze Kwalifikacji (ZRK), a także zasady i standardy certyfikowania kwalifikacji oraz zapewniania jakości nadawania kwalifikacji. Informacje o ZSK są dostępne pod adresem: https://www.kwalifikacje.gov.pl
Zintegrowany Rejestr Kwalifikacji (ZRK)	Rejestr publiczny prowadzony w systemie teleinformatycznym ewidencjonujący kwalifikacje włączone do Zintegrowanego Systemu Kwalifikacji. Informacje o ZRK są dostępne pod adresem: https://rejestr.kwalifikacje.gov.pl

7.2. Definicje związane z wykonywaniem zawodu (branżowe)

Lp.	Nazwa pojęcia	Definicja	Źródło
1	Certyfikowany audytor	Przeszkolona osoba posiadająca uprawnienia w zakresie danej normy, poprzez udział w szkoleniu, jak również odbyciu praktyk, które umożliwiają audytowanie procesów i uzyskiwanie dowodu z audytu oraz jego obiektywnej oceny, w celu określenia stopnia spełnienia kryteriów audytu z ramienia jednostek certyfikujących.	Pacana A., Stadnicka D.: Wdrażanie i auditowanie systemów zarządzania jakością zgodnych z normą ISO 9001:2000. Oficyna Wydawnicza Politechniki Rzeszowskiej, Rzeszów 2007
2	Czujnik produkcyjny	Urządzenie dostarczające informacje o pojawieniu się określonego bodźca, przekroczeniu pewnej wartości progowej.	Definicja opracowana przez zespół ekspercki na podstawie: http://yadda.icm.edu.pl/yadda/element/bwmeta1.element.baztech-7b406221-6db1-4221-936a-8589abb27f7d/c/78_198_TTS_T_KORNASZEWSKI_NOWAK.pdf [dostęp 31.10.2018]
3	Dane poufne	Właściwość polegająca na tym, że informacje nie są udostępniane lub wyjawiane nieupoważnionym osobom, podmiotom lub procesom.	PN-EN ISO/IEC 27001, Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji.
4	Dział IT	Dział przedsiębiorstwa lub innej organizacji odpowiedzialny za utrzymanie, usprawnienie i ewentualne rozwijanie wykorzystywanych w organizacji technologii informatycznych.	Definicja opracowana przez zespół ekspercki na podstawie: Tabakow M., Korczak J., Franczyk B.: Big data – definicje, wyzwania i technologie informatyczne. Informatyka Ekonomiczna, 2014
5	Dziennik zdarzeń/logi	Zapis komputerowy zawierający informacje o zdarzeniach i działaniach systemu informatycznego lub komputera.	Definicja opracowana przez zespół ekspercki na podstawie: https://sjp.pwn.pl/sjp/log-1;2566265.html [dostęp 31.10.2018]
6	Hurtownia danych	Rodzaj bazy danych przeznaczony do przechowywania informacji w długim horyzoncie czasowym. Oprogramowanie i sprzęt informatyczny połączony w zintegrowaną całość, zmieniającą się wraz z rozwojem technologii i gromadzeniem danych w przedsiębiorstwie.	Definicja opracowana przez zespół ekspercki na podstawie: https://mfiles.pl/pl/index.php/Hurtownia_danych [dostęp 31.10.2018]
7	Incydent	Pojedyncze zdarzenie lub seria niespodziewanych zdarzeń związanych z bezpieczeństwem informacji.	PN-EN ISO/IEC 27001, Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji.
8	Informacja	Aktywo biznesowe, które ma dla instytucji wartość i dlatego należy je odpowiednio chronić. Informacja może przybierać różne formy. Może być wydrukowana lub zapisana na papierze, przechowywana elektronicznie, przesyłana pocztą lub za pomocą urządzeń elektronicznych, wyświetlana w formie filmu, lub wypowiedzana w rozmowie.	PN-EN ISO/IEC 27002, Technika informatyczna – Techniki bezpieczeństwa – Praktyczne zasady zarządzania bezpieczeństwem informacji.

INFORMACJA O ZAWODZIE – Specjalista do spraw systemów zarządzania bezpieczeństwem informacji 252903

9	ISO (Międzynarodowa Organizacja Normalizacyjna)	Organizacja pozarządowa zrzeszająca krajowe instytucje zajmująca się opracowywaniem, tłumaczeniem z innych wersji językowych, przyjmowaniem i rozpowszechnianiem norm. Ang.: International Organization for Standardization.	https://www.iso.org [dostęp: 31.10.2018]
10	Jednostka kontrolna	Osoba lub zespół kontrolny, który jako instytucja niezależna od kontrolowanej organizacji, dostawcy i odbiorcy udziela pisemnego zapewnienia, że należyce zidentyfikowany wyrób, proces lub usługa są zgodne z określoną normą lub z właściwymi przepisami prawnymi.	PN-EN ISO/IEC 27001, Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji.
11	Kategoryzowanie informacji	Proces polegający na przydzieleniu do danej kategorii informacji mających podobny zestaw cech, w celu łatwiejszego nimi zarządzania.	Definicja opracowana przez zespół ekspercki na podstawie: https://sjp.pwn.pl/sjp/kategoryzacja;2563205.html [dostęp: 31.10.2018]
12	Klauzula poufności	Tajemnica przedsiębiorstwa rozumiana jako niepodane do wiadomości publicznej informacje techniczne, technologiczne, organizacyjne przedsiębiorstwa lub inne informacje posiadające wartość gospodarczą, co do których przedsiębiorca podjął niezbędne działania w celu zachowania ich poufności.	Ustawa z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji http://prawo.sejm.gov.pl/isap.nsf/download.xsp/WDU20180000419/U/D20180419Lj.pdf [dostęp: 31.10.2018]
13	Nadzór nad dokumentami i zapisami	Czynność wynikająca z normy systemu zarządzania, zobowiązująca do przestrzegania określonych czynności formalnych w postaci monitorowania dokumentów i ich zapisów.	Definicja opracowana przez zespół ekspercki na podstawie: https://mfiles.pl/pl/index.php/Nadz%C3%B3r_nad_dokumentami [dostęp: 31.10.2018]
14	Norma jakości	Zbiór wymagań znajdujących zastosowanie we wszystkich rodzajach organizacji.	PN-EN ISO/IEC 27001, Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji.
15	Osoby uprawnione	Osoba lub zespół mający prawo do zarządzania informacją według przyjętych reguł.	PN-EN ISO/IEC 27001, Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji.
16	Outsourcing	Powierzenie przez organizację realizacji określonego zadania usługodawcy przy jednoczesnym określeniu efektów, jakie zlecniodawca zamierza uzyskać, ale bez instrukcji dotyczących sposobu wykonywania poszczególnych zadań, pozostawiając inicjatywę w tym zakresie zlecnioobiorcy.	Definicja opracowana przez zespół ekspercki na podstawie: Trocki M.: Outsourcing: metoda restrukturyzacji działalności gospodarczej. PWE, Warszawa 2001
17	Polityka bezpieczeństwa	Ogół zasad, metod i narzędzi ochrony i nadzoru nad informacją. Obejmuje takie elementy, jak: polityka informacyjna, zasady ochrony danych osobowych, polityka bezpieczeństwa systemu teleinformatycznego, zasady ochrony tajemnicy przedsiębiorstwa lub innych tajemnic zawodowych, zapobieganie przestępstwom na szkodę firmy, szczególnie fałszerstwom i oszustwom, zasady ochrony fizycznej i technicznej oraz inne związane z bezpieczeństwem.	PN-EN ISO/IEC 27001, Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji.

INFORMACJA O ZAWODZIE – Specjalista do spraw systemów zarządzania bezpieczeństwem informacji 252903

18	Proces	Zbiór działań wzajemnie powiązanych lub wzajemnie oddziałujących, które przekształcają wejścia w wyjścia.	PN-EN ISO/IEC 27001, Technika informatyczna - Techniki bezpieczeństwa - Systemy zarządzania bezpieczeństwem informacji.
19	Protokoły internetowe	Zestaw technicznych uzgodnień określających sposób nawiązywania i prowadzenia komunikacji w Internecie.	Definicja opracowana przez zespół ekspercki na podstawie: https://encyklopedia.pwn.pl/haslo/protokol-komunikacyjny;3962902.html [dostęp: 31.10.2018]
20	Repozytorium informacyjne	Miejsce uporządkowanego przechowywania informacji, z których wszystkie przeznaczone są do udostępniania.	Definicja opracowana przez zespół ekspercki na podstawie: Owczarek K., Żurak-Owczarek, C.: Systemy informatyczne w zarządzaniu łańcuchem dostaw. Logistyka, nr 4/2015
21	Router	Aktywne urządzenie w sieci komputerowej, decydujące, jaką drogą mają być przesyłane dane.	https://sjp.pwn.pl/sjp/router;2574463.html [dostęp: 31.10.2018]
22	Strategia informacyjna przedsiębiorstwa	Całokształt długookresowych planów i działań, zmierzających do efektywnego wykorzystania różnorodnych narzędzi, środków i techniki dla osiągnięcia informacyjnych celów przedsiębiorstwa. Dostarcza informacje potrzebne do zrealizowania procesów i przedsięwzięć ekonomicznych oraz usprawnia obieg informacji, tj. częstość wykorzystania informacji, jakość, integralność i bezpieczeństwo informacji, decyzyjność informacji.	http://bazhum.muzhp.pl/media/files/Zarzadzanie_Zmianami_zeszyty_naukowe/Zarzadzanie_Zmianami_zeszyty_naukowe-r2011-t-n2/Zarzadzanie_Zmianami_zeszyty_naukowe-r2011-t-n2-s15-36/Zarzadzanie_Zmianami_zeszyty_naukowe-r2011-t-n2-s15-36.pdf [dostęp: 31.10.2018]
23	Szacowanie ryzyka	Całościowy proces analizy i oceny ryzyka.	PN-EN ISO/IEC 27001, Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji
24	Telepraca	Forma organizacji pracy polegająca na świadczeniu pracy zdalnie poza jednostką organizacyjną pracodawcy, za pomocą środków komunikacji elektronicznej.	Definicja opracowana przez zespół ekspercki na podstawie: Kryńska E. (red.): Elastyczne formy zatrudnienia i organizacji pracy a popyt na pracę w Polsce. IPiSS, Warszawa 2003 oraz Wróbel P.: Problemy zarządzania telepracownikami. Prace i materiały Wydziału Zarządzania Uniwersytetu Gdańskiego, Nr 2, 2007
25	Topologia sieci komputerowej	Określa relację pomiędzy urządzeniami w sieci komputerowej, połączenia między nimi oraz sposób przepływu danych.	Definicja opracowana przez zespół ekspercki na podstawie: https://egzamin-e13.pl/projektowanie-lokalnych-sieci-komputerowych-2/topologie-sieci-komputerowych [dostęp: 31.10.2018]

INFORMACJA O ZAWODZIE – Specjalista do spraw systemów zarządzania bezpieczeństwem informacji 252903

26	Właściciel procesu	Osoba odpowiedzialna za zapewnienie, by zarządzany proces był zgodny z przeznaczeniem. Do zakresu odpowiedzialności właściciela procesu należy sponsorowanie, projektowanie, zarządzanie zmianami oraz ustawiczne doskonalenie procesu i jego miar.	ITIL Foundation Handbook – Pocketbook from the Official Publisher of ITIL, TSO, 2012
27	Zadaniowy system pracy	Elastyczny rodzaj czasu pracy, w którym czas pracy pracownika mierzony jest wymiarem jego zadań.	https://kadry.infor.pl/popzednie_tematy_dnia/593542,Zasady-zatrudniania-w-zadaniowym-czasie-pracy.html [dostęp: 31.10.2018]

ZASTOSOWANIE INFORMACJI O ZAWODACH

Wsparcie dla pracowników i klientów instytucji rynku pracy w zakresie:

- skutecznego podejmowania decyzji dotyczących wyboru zawodu, pracy/zatrudnienia,
- nabywania nowych lub rozszerzania już posiadanych kompetencji zawodowych,
- zmiany kwalifikacji zawodowych zgodnie z potrzebami rynku pracy,
- dopasowywania treści szkoleń kontraktowanych przez urzędy pracy do potrzeb rynku pracy.

Wsparcie dla różnych grup interesariuszy w zakresie:

- poradnictwa i doradztwa zawodowego,
- tworzenia i aktualizacji ofert szkoleniowych dla rynku pracy,
- dostosowania oferty kształcenia zawodowego do wymagań rynku pracy,
- tworzenia i aktualizacji opisów stanowisk pracy,
- przygotowania lub aktualizacji opisu kwalifikacji rynkowych wprowadzanych do Zintegrowanego Systemu Kwalifikacji.