Fundusze Europejskie Wiedza Edukacja Rozwój
Rzeczpospolita Polska
INFOdoradca+
Unia Europejska Europejski Fundusz Społeczny

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 bezpieczeństwa systemów teleinformatycznych

(252902)

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 bezpieczeństwa systemów teleinformatycznych

(252902)

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 bezpieczeństwa systemów teleinformatycznych (252902)

ISBN 978-83-7789-495-8 [183]

Publikacja bezpłatna

Zdjęcie na okładce (źródło): https://pixabay.com/en/programming-developing-startup-593312 [dostęp: 31.03.2019].

SPIS TREŚCI

1. DANE IDENTYFIKACYJNE ZAWODU

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

Specjalista bezpieczeństwa systemów teleinformatycznych 252902

1.2. Nazwy zwyczajowe zawodu

- Administrator zarządzania bezpieczeństwem IT.
- Specjalista ds. bezpieczeństwa informatycznego.
- Specjalista ds. cyberbezpieczeństwa.
- Specjalista ds. IT.

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 Wortalu Publicznych Służb Zatrudnienia,
- badań ankietowych prowadzonych w projekcie INFODORADCA+ w marcu 2019 r.,
- zebranych opinii od recenzentów, członków panelu ewaluacyjnego oraz zespołu ds. walidacji i jakości informacji o zawodach.

Autorzy i eksperci opiniujący

Zespół Ekspercki:

- Włodzimierz Walkusz – DORADCA Consultants Ltd. sp. z o.o., Gdynia.
- Paweł Weichbroth – Memex Paweł Weichbroth, Gdańsk.
- Artur Wróblewski – Ekspert niezależny, Częstochowa.

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.
- Krzysztof Symela – Instytut Technologii Eksploatacji – PIB, Radom.
- Ireneusz Woźniak – Instytut Technologii Eksploatacji – PIB, Radom.

Recenzenci:

- Jakub Bieszke – InterLAN sp. z o.o. sp. k., Poznań.
- Damian Rusek – RADMOT sp. z o.o. sp. k., Radom.

Panel ewaluacyjny – przedstawiciele partnerów społecznych:

- Radosław Niemczewski – Centrum Kształcenia Praktycznego, Pleszew.
- Dariusz Tomczak – Zespół Szkół Elektrycznych im. prof. Janusza Groszkowskiego w Białymstoku, Białystok.

Data (rok) opracowania opisu informacji o zawodzie: 2019 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 bezpieczeństwa systemów teleinformatycznych[19] zajmuje się zapewnianiem ochrony systemów elektronicznych i urządzeń końcowych[21], głównie komputerów i sieci komputerowych, przed niepożądanym dostępem i manipulacją przez osoby trzecie lub przed nieprawidłowym użytkowaniem tych systemów przez użytkowników. Realizuje to zadanie poprzez rozwój i wdrażanie zabezpieczeń technicznych i organizacyjnych zarówno na poziomie używanych w tych systemach urządzeń, jak i zastosowanego oprogramowania.

2.2. Opis pracy i sposobu jej wykonywania

Opis pracy

Celem pracy w zawodzie **specjalista bezpieczeństwa systemów teleinformatycznych** jest osiągnięcie i stałe utrzymywanie bezpieczeństwa pracy tych systemów. Cel ten obejmuje zapewnienie poufności i dostępności wykorzystywanych, przetwarzanych i przesyłanych danych. Dane te muszą być zabezpieczone przed usunięciem (celowym lub nieświadomym), manipulacją oraz dostępem do nich przez osoby niepożądane.

Specjalista bezpieczeństwa systemów teleinformatycznych zajmuje się opracowywaniem zabezpieczeń urządzeń elektronicznych lub oprogramowania oraz wdrażaniem i dopasowywaniem gotowych rozwiązań zabezpieczających do wymagań systemów teleinformatycznych. Odpowiada on za aktualizację i dostosowywanie do aktualnego stanu zagrożeń, zasad bezpieczeństwa zaimplementowanych[8] w systemach teleinformatycznych. Przeprowadza również analizy systemów w zakresie bezpieczeństwa teleinformatycznego i ich odporności na cyberataki[5].

Sposoby wykonywania pracy

Praca **specjalisty bezpieczeństwa systemów teleinformatycznych** odbywa się przez większość czasu w interakcji z komputerem i polega m.in. na:

- monitorowaniu aktywności systemów teleinformatycznych,
- rozwiązywaniu problemów związanych z incydentami[9] zagrożenia bezpieczeństwa,
- aktualizowaniu i wprowadzaniu nowych zabezpieczeń w sferze oprogramowania i sprzętu,
- sprawdzaniu efektywności wprowadzonych rozwiązań,
- monitorowaniu pojawiających się w różnych źródłach, informacji o cyberatakach oraz o powstawaniu nowych form cyberataków,
- niezwłocznym przeciwdziałaniu zagrożeniom bezpieczeństwa systemów teleinformatycznych,
- monitorowaniu ogólnej efektywności struktury systemów teleinformatycznych,
- dokumentowaniu w formie raportów okresowych, pracy systemu z zastosowaniem przyjętych standardów.

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

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

Warunki pracy

Stanowisko pracy **specjalisty bezpieczeństwa systemów teleinformatycznych** znajduje się na ogół w dobrze oświetlonych, często klimatyzowanych pomieszczeniach i wyposażone jest w sprzęt komputerowy. Praca wykonywana jest w pozycji siedzącej.

W zależności od struktury obsługiwanego systemu komputerowego, specjalista bezpieczeństwa systemów teleinformatycznych wykonuje zadania zawodowe w pomieszczeniach, w których znajdują się stacje robocze[18], a także w serwerowniach[17] lub innych pomieszczeniach, w których pracują serwery[16] i urządzenia sieciowe. W pomieszczeniach tych może występować podwyższony poziom hałasu.

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

Wykorzystywane maszyny i narzędzia pracy

Specjalista bezpieczeństwa systemów teleinformatycznych w działalności zawodowej wykorzystuje m.in.:
- serwery komputerowe,
- stacje robocze,
- urządzenia sieciowe,
- oprogramowanie systemowe[13],
- oprogramowanie narzędziowe[12],
- oprogramowanie antywirusowe[11],
- oprogramowanie użytkowe[14],
- urządzenia specjalistyczne, w przypadku inspekcji zabezpieczeń na poziomie infrastruktury fizycznej,
- urządzenia peryferyjne (np. drukarkę),
- telefon,
- samochód,
- sprzęt do prezentacji multimedialnej.

Organizacja pracy

Specjalista bezpieczeństwa systemów teleinformatycznych:
- pracuje zwykle w systemie jednozmianowym,
- pracuje często w godzinach nadliczbowych,
- może mieć elastyczny czas pracy.

Częściowo możliwe jest wykonywanie niektórych zadań zawodowych poprzez dostęp zdalny[7] (w systemie telepracy) z dowolnego miejsca. Podróże służbowe możliwe są przede wszystkim w przypadku przeprowadzania audytów bezpieczeństwa systemów teleinformatycznych. W przypadku współpracy z zagranicznymi firmami może zachodzić konieczność dostosowania czasu pracy do właściwej strefy czasowej.

Specjalista bezpieczeństwa systemów teleinformatycznych:
- pracuje często samodzielnie,
- w przypadku bardziej złożonych systemów lub dużych organizacji może pracować zespołowo,

- w zależności od zajmowanego stanowiska, może pracować pod nadzorem lub zarządzać zespołem,
- ściśle współpracuje z administratorem systemów teleinformatycznych.

Kontaktuje się m.in. z użytkownikami systemów teleinformatycznych oraz innymi specjalistami odpowiedzialnymi za obszar informatyki (np. audytorzy[4], dostawcy usług informatycznych).

Poszczególne systemy teleinformatyczne różnią się od siebie, a nowe formy cyberataków powstają nieustannie. Wymaga to ciągłego poszerzania swojej wiedzy, dlatego praca ma charakter nierutynowy i niemonotonny, a środowisko pracy należy uznać za zmienne.

Specjaliści bezpieczeństwa systemów teleinformatycznych zatrudniani są najczęściej w oparciu o umowę o pracę, jednak coraz częściej spotykaną formą jest samozatrudnienie.

Zagrożenia mające wpływ na bezpieczeństwo pracy człowieka

Wykonywanie pracy w zawodzie **specjalista bezpieczeństwa systemów teleinformatycznych** nie wiąże się z występowaniem specyficznych zagrożeń dla zdrowia, poza typowymi związanymi z pracą siedzącą przy monitorze komputera, takimi jak:

- pogorszenie wzroku,
- choroby narządu ruchu (są to przede wszystkim zmiany na odcinku szyjnym kręgosłupa),
- zmiany w układzie kostno-stawowym (w szczególności w nadgarstkach),
- schorzenia związane ze stresem i pracą pod presją czasu.

2.4. Wymagania psychofizyczne i zdrowotne

Wymagania psychofizyczne

Dla pracownika wykonującego zawód **specjalista bezpieczeństwa systemów teleinformatycznych** ważne są:

w kategorii wymagań fizycznych

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

w kategorii sprawności sensomotorycznych

- ostrość słuchu,
- ostrość wzroku,
- koordynacja wzrokowo-ruchowa,
- spostrzegawczość,
- zręczność rąk,
- zręczność palców;

w kategorii sprawności i zdolności

- dobra organizacja pracy własnej,
- zdolność koncentracji uwagi,
- rozumowanie logiczne,
- podzielność uwagi,
- współdziałanie i współpraca w zespole (grupie),
- uzdolnienia techniczne;

w kategorii cech osobowościowych

- wytrwałość i cierpliwość,
- dokładność,

- dyskrecja,
- kreatywne podejście do rozwiązywania problemów,
- elastyczność i otwartość na zmiany,
- radzenie sobie ze stresem,
- gotowość do pracy indywidualnej,
- gotowość do współdziałania,
- samodzielność,
- samodyscyplina,
- dbałość o jakość pracy,
- zainteresowania informatyczne,
- gotowość do ustawicznego uczenia się.

Więcej informacji znajduje się w sekcjach*: *3.4. Kompetencje społeczne; 3.5. Profil kompetencji kluczowych dla zawodu.

Wymagania zdrowotne

Do pracy w zawodzie **specjalista bezpieczeństwa systemów teleinformatycznych** wymagany jest ogólny dobry stan zdrowia, prawidłowy wzrok oraz zręczność rąk i palców. Pod względem wydatku energetycznego praca w tym zawodzie należy do prac lekkich. W pracy występują specyficzne obciążenia umysłowe: rozwiązywanie problemów, analizowanie, wnioskowanie, wyjaśnianie, rozumowanie logiczne, wyobraźnia i myślenie twórcze.

Do przeciwwskazań uniemożliwiających pracę w zawodzie specjalista bezpieczeństwa systemów teleinformatycznych można zaliczyć:
- wady wzroku w stopniu uniemożliwiającym korekcję za pomocą okularów,
- dysfunkcje kończyn dolnych, jak i górnych, o ile ograniczają możliwość długotrwałej pracy przy komputerze, możliwości chodzenia i stania.

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

Obecnie (2019 r.) do podjęcia pracy w zawodzie **specjalista bezpieczeństwa systemów teleinformatycznych** preferowane jest wykształcenie wyższe co najmniej I stopnia na kierunku informatyka, informatyka stosowana, informatyka i ekonometria, telekomunikacja, elektronika lub pokrewnym, najlepiej ze specjalnością bezpieczeństwo systemów informatycznych, kryptologia lub cyberbezpieczeństwo[6] oraz na kierunkach łączących matematykę z różnymi specjalnościami informatycznymi lub studia podyplomowe z zakresu bezpieczeństwa informacji.

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

Podjęcie pracy w zawodzie **specjalista bezpieczeństwa systemów teleinformatycznych** ułatwia posiadanie dyplomu ukończenia studiów wyższych (studia I i II stopnia) oraz studiów podyplomowych na kierunkach: informatyka, informatyka stosowana, informatyka i ekonometria, telekomunikacja, elektronika lub pokrewnym, najlepiej ze specjalnością bezpieczeństwo systemów informatycznych, kryptologia lub cyberbezpieczeństwo oraz na kierunkach łączących matematykę z różnymi specjalnościami informatycznymi lub studiów podyplomowych z zakresu bezpieczeństwa informacji.

Dodatkowymi atutami przy zatrudnianiu mogą być zaświadczenia/certyfikaty potwierdzające kwalifikacje specjalisty, np. w zakresie:
- bardzo dobrej znajomości obsługi komputera,
- obsługi specjalistycznego oprogramowania służącego do zabezpieczania komputerów i systemów informatycznych przed cyberatakami,
- języka angielskiego w stopniu komunikatywnym w zakresie czytania dokumentów,
- metodyki prowadzenia analiz i rozwiązywania problemów w zakresie bezpieczeństwa systemów teleinformatycznych,
- kryptografii,
- zarządzania wymaganiami oraz zarządzania zmianą,
- systemów zarządzania bezpieczeństwem informacji ISO 27001.

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

Specjalista bezpieczeństwa systemów informatycznych jest zawodem rozpoczynającym karierę osób poświęcających się cyberbezpieczeństwu. Po zdobyciu doświadczenia możliwa jest praca jako:
- konsultant ds. bezpieczeństwa IT lub tester zabezpieczeń IT (Penetration Tester),
- ekspert ds. bezpieczeństwa IT lub ekspert ds. cyberbezpieczeństwa (Security Officer),
- menedżer ds. cyberbezpieczeństwa lub dyrektor bezpieczeństwa informacji,
- audytor bezpieczeństwa po zdaniu egzaminu na certyfikowanego audytora ISO 27001.

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 (2019 r.) w zawodzie **specjalista bezpieczeństwa systemów teleinformatycznych** możliwości potwierdzania kompetencji zawodowych w edukacji formalnej ograniczają się do studiów na kierunku informatyka, informatyka stosowana, informatyka i ekonometria, telekomunikacja, elektronika lub pokrewnym, najlepiej ze specjalnością bezpieczeństwo systemów informatycznych, kryptologia lub cyberbezpieczeństwo, na kierunkach łączących matematykę z różnymi specjalnościami informatycznymi oraz studiów podyplomowych z zakresu bezpieczeństwa informacji.

Specjalista bezpieczeństwa systemów teleinformatycznych może potwierdzać również kompetencje certyfikatami i dyplomami z ukończonych specjalistycznych szkoleń z zakresu konfiguracji sieciowych systemów operacyjnych i urządzeń sieciowych oraz bezpieczeństwa informacji. Jednymi z najistotniejszych w zawodzie są certyfikaty potwierdzające:
- znajomość normy ISO/IEC 27001,
- wiedzę i praktyczne doświadczenie z zakresu technologii sieciowych i konfiguracji systemów operacyjnych Windows i Linux.

Ponadto możliwością potwierdzenia kompetencji jest uzyskanie referencji z poprzednich miejsc pracy.

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 bezpieczeństwa systemów teleinformatycznych** może rozszerzać swoje kompetencje zawodowe w zawodach pokrewnych:

Nazwa zawodu pokrewnego zgodnie z Klasyfikacją zawodów i specjalności	Kod zawodu
Konsultant do spraw systemów teleinformatycznych	251102
Projektant / architekt systemów teleinformatycznych	251103
Specjalista bezpieczeństwa oprogramowania	252901
Specjalista do spraw systemów zarządzania bezpieczeństwem informacji	252903

3. ZADANIA ZAWODOWE I WYMAGANE KOMPETENCJE

3.1. Zadania zawodowe

Pracownik w zawodzie **specjalista bezpieczeństwa systemów teleinformatycznych** wykonuje różnorodne zadania, do których należą w szczególności:

Z1 Monitorowanie bieżącej aktywności i bezpieczeństwa systemów teleinformatycznych.
Z2 Prowadzenie stałego i okresowego przeglądu logów[10] systemów teleinformatycznych.
Z3 Sporządzanie i prezentowanie raportów okresowych w zakresie aktywności i bezpieczeństwa systemów teleinformatycznych.
Z4 Diagnozowanie incydentów bezpieczeństwa systemów teleinformatycznych.
Z5 Rozwiązywanie i zgłaszanie incydentów bezpieczeństwa systemów teleinformatycznych.
Z6 Opracowywanie planów przeciwdziałania incydentom bezpieczeństwa.
Z7 Wdrażanie planów przeciwdziałania incydentom bezpieczeństwa.
Z8 Analizowanie, przygotowywanie i utrzymywanie dokumentacji w zakresie bezpieczeństwa systemów teleinformatycznych.

3.2. Kompetencja zawodowa Kz1: Monitorowanie i raportowanie w zakresie bezpieczeństwa systemów teleinformatycznych

Kompetencja zawodowa Kz1: Monitorowanie i raportowanie w zakresie bezpieczeństwa systemów teleinformatycznych obejmuje zestaw zadań zawodowych Z1, Z2, Z3, do realizacji których wymagane są odpowiednie zbiory wiedzy i umiejętności.

Z1 Monitorowanie bieżącej aktywności i bezpieczeństwa systemów teleinformatycznych	
WIEDZA – zna i rozumie:	**UMIEJĘTNOŚCI – potrafi:**
• Istotę, założenia i cele monitorowania systemów teleinformatycznych; • Źródła danych, rodzaj i typ danych opisujących bieżącą aktywność i stan sieci komputerowej oraz systemów teleinformatycznych; • Sposób działania urządzeń sieciowych stosowanych w sieciach komputerowych; • Architekturę[3] oraz specyfikę działania systemów teleinformatycznych; • Funkcjonalność systemów i narzędzi informatycznych stosowanych do monitorowania bieżącej aktywności i stanu sieci komputerowej.	• Definiować obszar i cele monitorowania systemów teleinformatycznych; • Analizować dane opisujące bieżącą aktywność i stan sieci komputerowej oraz systemów teleinformatycznych; • Monitorować działanie urządzeń sieciowych stosowanych w sieciach komputerowych; • Monitorować działanie systemów teleinformatycznych; • Wykorzystywać systemy i narzędzia informatyczne do monitorowania bieżącej aktywności i stanu sieci komputerowej.

Z2 Prowadzenie stałego i okresowego przeglądu logów systemów teleinformatycznych	
WIEDZA – zna i rozumie:	**UMIEJĘTNOŚCI – potrafi:**
• Źródła danych na temat zdarzeń w systemach teleinformatycznych, gromadzonych w plikach logów systemowych; • Techniki i metody poszukiwania, grupowania i wyświetlania danych tekstowych w logach systemowych; • Narzędzia podglądu logów systemowych.	• Analizować oraz interpretować dane pochodzące z logów systemowych; • Wyszukiwać, grupować i wyświetlać dane, biorąc pod uwagę format ich zapisu; • Posługiwać się narzędziami do podglądu logów systemowych.

Z3 Sporządzanie i prezentowanie raportów okresowych w zakresie aktywności i bezpieczeństwa systemów teleinformatycznych	
WIEDZA – zna i rozumie:	**UMIEJĘTNOŚCI – potrafi:**
• Techniki eksportu oraz importu danych do i z programów służących analizie danych; • Składniki i pozycje raportu bezpieczeństwa systemów teleinformatycznych; • Narzędzia do przygotowywania raportów okresowych, dotyczących stopnia aktywności i stanu systemów teleinformatycznych; • Narzędzia i techniki prezentacji danych dotyczących wykorzystania i bezpieczeństwa systemów teleinformatycznych.	• Eksportować oraz importować dane do i z systemu oraz narzędzi raportowania; • Analizować, interpretować, agregować[1] oraz filtrować dane na potrzeby przygotowywania sprawozdań i raportów okresowych z aktywności i bezpieczeństwa systemów teleinformatycznych; • Wykorzystywać narzędzia do sporządzania raportów dotyczących stopnia aktywności i bezpieczeństwa systemów teleinformatycznych; • Wykorzystywać narzędzia i techniki prezentacji danych dotyczących wykorzystania i bezpieczeństwa systemów teleinformatycznych.

3.3. Kompetencja zawodowa Kz2: Zarządzanie incydentami bezpieczeństwa systemów teleinformatycznych

Kompetencja zawodowa Kz2: Zarządzanie incydentami bezpieczeństwa systemów teleinformatycznych obejmuje zestaw zadań zawodowych Z4, Z5, Z6, Z7, Z8, do realizacji których wymagane są odpowiednie zbiory wiedzy i umiejętności.

Z4 Diagnozowanie incydentów bezpieczeństwa systemów teleinformatycznych	
WIEDZA – zna i rozumie:	**UMIEJĘTNOŚCI – potrafi:**
• Definicje i pojęcia zdarzeń w zakresie naruszenia bezpieczeństwa aktywów informacyjnych[2] organizacji; • Techniki identyfikacji incydentów bezpieczeństwa; • Źródła i rodzaje ataków na systemy teleinformatyczne stanowiących incydenty bezpieczeństwa.	• Analizować zdarzenia naruszające bezpieczeństwo aktywów informacyjnych organizacji; • Stosować i wdrażać techniki identyfikacji incydentów bezpieczeństwa; • Oceniać i selekcjonować informacje na temat zidentyfikowanego incydentu bezpieczeństwa.

Z5 Rozwiązywanie i zgłaszanie incydentów bezpieczeństwa systemów teleinformatycznych	
WIEDZA – zna i rozumie:	**UMIEJĘTNOŚCI – potrafi:**
• Techniki i metody eliminacji i ograniczania zasięgu szkodliwych skutków zaistniałych incydentów bezpieczeństwa; • Techniki i mechanizmy kontroli i weryfikacji bieżącego stanu systemów teleinformatycznych po usunięciu incydentów bezpieczeństwa; • Proces i sposób opisu zgłaszanych incydentów bezpieczeństwa.	• Eliminować i ograniczać zasięg szkodliwych skutków zaistniałych incydentów bezpieczeństwa na działalność organizacji; • Kontrolować i weryfikować bieżący stan systemów teleinformatycznych po usunięciu incydentów bezpieczeństwa; • Opisywać i zgłaszać incydenty bezpieczeństwa.

Z6 Opracowywanie planów przeciwdziałania incydentom bezpieczeństwa	
WIEDZA – zna i rozumie:	**UMIEJĘTNOŚCI – potrafi:**
• Źródła ryzyka[15] i zagrożeń bezpieczeństwa systemów teleinformatycznych; • Zabezpieczenia stosowane w zakresie utrzymania bezpieczeństwa systemów teleinformatycznych; • Zasady i techniki projektowania systemów wykrywania i zapobiegania naruszeniom[20] po stronie organizacji oraz użytkowników końcowych; • Cele, założenia i procesy dotyczące bezpieczeństwa systemów teleinformatycznych organizacji; • Stosowane rozwiązania, normy standaryzujące oraz inne powiązane akty prawne w zakresie ochrony informacji.	• Identyfikować i oceniać źródła ryzyka i zagrożeń w zakresie bezpieczeństwa systemów teleinformatycznych; • Identyfikować i oceniać zabezpieczenia systemów teleinformatycznych pod kątem ich kompletności i poprawności; • Projektować systemy wykrywania i zapobiegania naruszeń po stronie organizacji oraz użytkowników końcowych; • Tworzyć strategię, standardy oraz instrukcje bezpieczeństwa dla systemów teleinformatycznych organizacji; • Współpracować z dostawcami i audytorami bezpieczeństwa systemów teleinformatycznych.

Z7 Wdrażanie planów przeciwdziałania incydentom bezpieczeństwa	
WIEDZA – zna i rozumie:	**UMIEJĘTNOŚCI – potrafi:**
• Sposób działania rozwiązań i mechanizmów detekcji naruszeń i ochrony bezpieczeństwa systemów teleinformatycznych, po stronie organizacji oraz użytkowników końcowych; • Techniki wdrażania rozwiązań i mechanizmów detekcji naruszeń i ochrony bezpieczeństwa po stronie organizacji oraz użytkowników końcowych; • Ograniczenia, uwarunkowania i kryteria oceny działania rozwiązań i mechanizmów detekcji naruszeń i ochrony bezpieczeństwa po stronie organizacji oraz użytkowników końcowych.	• Organizować i planować wdrażanie rozwiązań i mechanizmów detekcji naruszeń i ochrony bezpieczeństwa systemów teleinformatycznych po stronie organizacji oraz użytkowników końcowych; • Wdrażać rozwiązania i mechanizmy detekcji naruszeń i ochrony bezpieczeństwa po stronie organizacji oraz użytkowników końcowych; • Kontrolować i korygować działanie rozwiązań i mechanizmów detekcji naruszeń i ochrony bezpieczeństwa po stronie organizacji oraz użytkowników końcowych.

Z8 Analizowanie, przygotowywanie i utrzymywanie dokumentacji w zakresie bezpieczeństwa systemów teleinformatycznych	
WIEDZA – zna i rozumie:	**UMIEJĘTNOŚCI – potrafi:**
• Definicje, pojęcia, normy standaryzujące oraz przepisy prawa w obszarze bezpieczeństwa systemów teleinformatycznych; • Źródła informacji dostępne w dokumentacji oraz internecie dotyczące rozwiązań i mechanizmów detekcji naruszeń i ochrony bezpieczeństwa po stronie organizacji oraz użytkowników końcowych; • Metody opisu celów, założeń, standardów, procesów oraz instrukcji w zakresie rozwiązań i mechanizmów detekcji naruszeń i ochrony bezpieczeństwa systemów teleinformatycznych; • Proces kosztorysowania i nośniki kosztów procesu bezpieczeństwa teleinformatycznego.	• Analizować oraz interpretować zapisy dokumentacji, norm standaryzujących i przepisów prawa w zakresie bezpieczeństwa systemów teleinformatycznych; • Wyszukiwać w dokumentacji oraz w internecie niezbędne informacje dotyczące specyfikacji rozwiązań i mechanizmów detekcji naruszeń i ochrony bezpieczeństwa po stronie organizacji oraz użytkowników końcowych; • Opisywać cele, założenia, standardy, procesy oraz instrukcje obejmujące istniejące rozwiązania i mechanizmy detekcji naruszeń i ochrony bezpieczeństwa systemów teleinformatycznych; • Identyfikować nośniki i szacować koszty procesu bezpieczeństwa teleinformatycznego.

3.4. Kompetencje społeczne

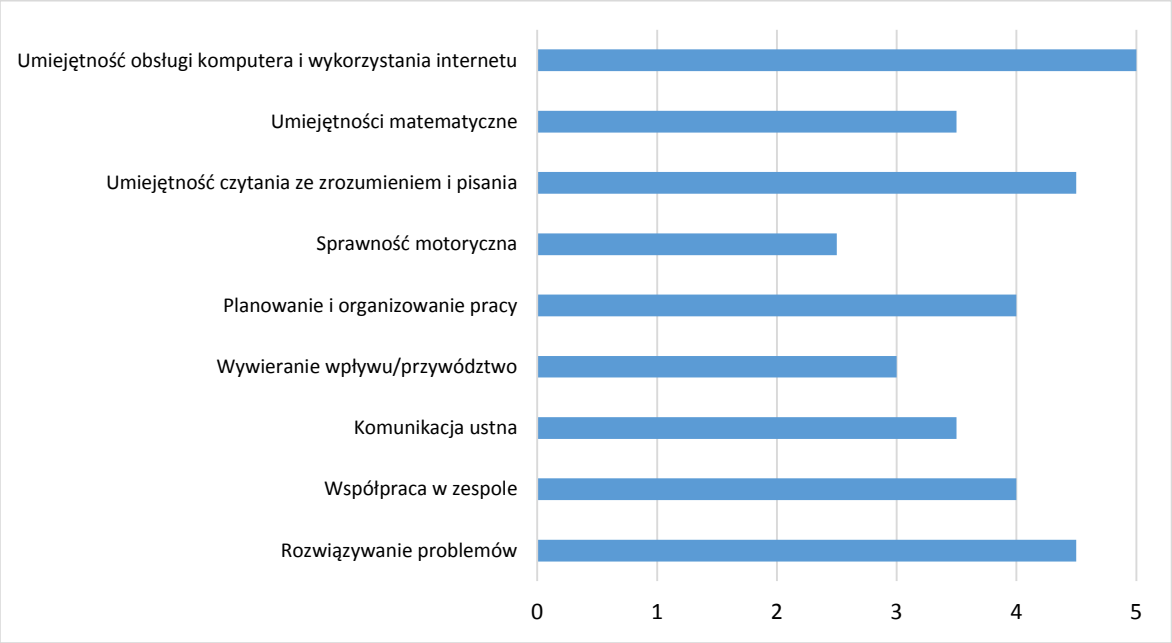
Pracownik w zawodzie **specjalista bezpieczeństwa systemów teleinformatycznych** powinien posiadać kompetencje społeczne niezbędne do prawidłowego i skutecznego wykonywania zadań zawodowych.

W szczególności pracownik jest gotów do:

- Przyjmowania odpowiedzialności za skutki działalności zawodowej ze świadomością ich efektów społecznych i gospodarczych oraz konsekwencji prawnych.
- Działania zgodnie z obowiązującym prawem, standardami, procedurami i zasadami etyki zawodowej w zakresie zapewniania bezpieczeństwa systemów teleinformatycznych.
- Promowania zasad etycznych w dziedzinie bezpieczeństwa systemów teleinformatycznych.
- Zachowywania tajemnicy zawodowej związanej z dostępem do informacji poufnych w systemach teleinformatycznych.
- Przestrzegania obowiązujących w działalności zawodowej zasad postępowania gwarantujących właściwą jakość działań zawodowych oraz bezpieczeństwa systemów teleinformatycznych.
- Dokonywania oceny jakości dostarczanych przez siebie usług w aspekcie merytorycznym i ekonomicznym oraz do poddawania się takiej ocenie.
- Poszukiwania rozwiązań zwiększających efektywność i podnoszących jakość wykonywanej przez siebie pracy.
- Funkcjonowania w zespole ze świadomością, jak ważne jest w pracy zespołowej poszanowanie różnorodności poglądów i kultur oraz świadomością wpływu wykonywanych przez siebie zadań na efekty pracy zespołu.
- Utrzymywania właściwych relacji w środowisku zawodowym związanym z zapewnianiem bezpieczeństwa systemów teleinformatycznych.

3.5. 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 ważność kompetencji kluczowych dla zawodu **specjalista bezpieczeństwa systemów teleinformatycznych.**



Rys. 1. Profil kompetencji kluczowych dla zawodu **specjalista bezpieczeństwa systemów teleinformatycznych**

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

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

Kompetencje zawodowe pracownika w zawodzie **specjalista bezpieczeństwa systemów teleinformatycznych** 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 bezpieczeństwa systemów teleinformatycznych może znaleźć zatrudnienie m.in. w:

- działach IT przedsiębiorstw we wszystkich dziedzinach gospodarki,
- firmach informatycznych,
- bankach,

- placówkach badawczo-rozwojowych,
- placówkach służby zdrowia,
- szkołach i uczelniach,
- policji, wojsku, straży granicznej,
- innych instytucjach administracji państwowej.

Obecnie (2019 r.) odnotowuje się w Polsce deficyt pracowników w branży IT, a zapotrzebowanie na specjalistów od cyberbezpieczeństwa jest szczególnie wysokie. Branża rozwija się bardzo dynamicznie, co objawia się tym, że osoby z odpowiednimi kompetencjami nie mają problemów ze znalezieniem dobrze płatnej pracy.

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: 31.03.2019]:
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-rynku-pracya
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 (2019 r.) do pracy w zawodzie **specjalista bezpieczeństwa systemów teleinformatycznych** przygotowują w Polsce liczne szkoły wyższe na studiach I i II oraz III stopnia na kierunkach:

- bezpieczeństwo systemów informatycznych,
- informatyka,
- informatyka stosowana,

- informatyka i ekonometria,
- telekomunikacja,
- elektronika,
- kryptologia i cyberbezpieczeństwo,
- matematyka w połączeniu z różnymi specjalnościami informatycznymi.

Kształcenie na tych kierunkach oferują 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

Rynek oferuje szeroki zakres szkoleń branżowych, na których **specjalista bezpieczeństwa systemów teleinformatycznych** może poszerzyć swoją wiedzę. W związku z obserwowanym gwałtownym skokiem technologicznym w dziedzinie teleinformatyki wymagane jest stałe doskonalenie się, aby posiadać aktualną wiedzę na temat rozwijających i zmieniających się technologii.

Specjalista bezpieczeństwa systemów teleinformatycznych ma do wyboru ofertę wielu instytucji organizujących certyfikowane szkolenia uznawane przez międzynarodowe przedsiębiorstwa. Certyfikaty ukończenia tych szkoleń potwierdzają znajomość zagadnień z zakresu bezpieczeństwa systemów teleinformatycznych. W szerokiej gamie uznanych kursów oferowanych np. przez producentów systemów bezpieczeństwa lub oprogramowania, głównie jednak przez niezależne organizacje akredytacyjne, można wymienić m.in.:

- Security+,
- CERT Information Security Professional Certificate,
- CompTIA CSA+,
- CCSA Check Point Certified Security Administrator,
- CCNA Security,
- NSE 4 – FortiGate Network Security Professional,
- CISSP Certified Information Systems Security Professional,
- CISM Certified Information Security Manager,
- CPTE Certified Penetration Testing Engineer.

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: 31.03.2019]:

Szkolnictwo wyższe:
www.wybierzstudia.nauka.gov.pl

Szkolnictwo zawodowe:
https://www.ore.edu.pl/category/ksztalcenie-zawodowe-i-ustawiczne
http://doradztwo.ore.edu.pl/wybieram-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 (2019 r.) osób pracujących w zawodzie **specjalista bezpieczeństwa systemów teleinformatycznych** waha się najczęściej od 5000 zł do 14 000 zł brutto miesięcznie w przeliczeniu na pełen etat. Większość specjalistów osiąga zarobki w dolnej części podanego przedziału wynagrodzenia (mediana zarobków wynosi około 7900 zł brutto miesięcznie).

Zarobki specjalisty bezpieczeństwa systemów teleinformatycznych zależą od wielkości firmy, pochodzenia jej kapitału, posiadanego wykształcenia i stażu pracy, regionu zatrudnienia oraz wielkości miejscowości pracodawcy. W administracji publicznej zarobki mogą być nawet o 30% niższe.

Wartość wynagrodzeń brutto miesięcznie (ramowo) waha się w zależności od stażu pracy:
- od 2 do 3 lat – 5800 zł,
- od 4 do 5 lat – 7200 zł,
- od 6 lat – 8300 zł.

Dodatkowo standardem wśród wielu przedsiębiorstw jest oferowanie pracującym w zawodzie dodatkowych, pozapłacowych benefitów m.in.:
- prywatna opieka medyczna,
- karnet sportowy,
- ubezpieczenie na życie,
- dofinansowanie nauki i kursów językowych,
- możliwość pracy zdalnej.

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: 31.03.2019]:
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-szczeblach
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 bezpieczeństwa systemów teleinformatycznych** możliwe jest zatrudnienie osób niepełnosprawnych.

Warunkiem niezbędnym do zatrudnienia osób z niepełnosprawnościami w zawodzie 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, wymagane jest wówczas dostosowanie sprzętu komputerowego,
- z niewielką dysfunkcją kończyn dolnych (05-R), wymagane jest wówczas wyposażenie stanowiska w uchwyty, poręcze, regulowaną wysokość krzesła, podnóżka i inne udogodnienia,
- poruszające się na wózkach inwalidzkich (05-R), wymagany jest wówczas odpowiedni dobór stanowiska bądź ograniczenie lub zmodyfikowanie zakresu pracy w celu umożliwienia wykonywania zadań w pozycji siedzącej, zalecana jest praca biurowa lub koncepcyjna,

- z wadami i dysfunkcją wzroku (04-O), w przypadku możliwości skorygowania ich szkłami optycznymi lub soczewkami kontaktowymi,
- z dysfunkcją narządu słuchu (03-L), pod warunkiem, że niepełnosprawność ta jest możliwa do skorygowania za pomocą aparatów słuchowych,
- z dysfunkcją sfery psychicznej (02-P), pod warunkiem, że praca, poza wyjątkowymi sytuacjami (wyjazdy, sytuacje kryzysowe w firmie), nie zaburza rytmu dnia i nocy pracownika i zachowana jest zasada równego traktowania pracowników,
- z epilepsją (06-E), pod warunkiem, że napady padaczkowe występują sporadycznie i są sygnalizowane przez aurę, występują głównie wieczorem lub w nocy, nie powodują zbytniego zmęczenia i stosunkowo szybko następuje regeneracja sił po ich wystąpieniu, a przebieg choroby nie prowadzi do charakteropatii padaczkowej. Mogą być one zatrudnione warunkowo, po racjonalnym ograniczeniu zakresu zadań do sytuacji, w których możliwy jest stały nadzór i ewentualna szybka pomoc, a stanowisko pracy nie stwarza potencjalnych zagrożeń w przypadku emisji choroby,
- 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 i dokonywania niezbędnych zabiegów pielęgnacyjno-medycznych (np. zastrzyków insulinowych).

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 (2019 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: 31.03.2019 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 2018 r. poz. 2153, 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 16 lipca 2004 r. Prawo telekomunikacyjne (t.j. Dz. U. z 2018 r. poz. 1954, 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.).
- 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).

Literatura branżowa:

- Agutter C.: ITIL Foundation Handbook – Pocketbook from the Official Publisher of ITIL, 3RD Edition. The Stationery Office, 2012.
- Banaszak Z., Kłos S., Mleczko J.: Zintegrowane systemy informatyczne. PWE, Warszawa 2011.
- Dixit Avinash K.: Myślenie Strategiczne. Helion, Gliwice 2009.
- PN-EN ISO/IEC 27001, Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji. PKN, Warszawa 2017.
- Proctor T.: Twórcze rozwiązywanie problemów. GWP, Gdańsk 2002.
- Ryza S., Laserson U.: Spark. Zaawansowana analiza danych. Helion, Gliwice 2015.
- Sienkiewicz P. (red.): Inżynieria systemów bezpieczeństwa. PWE, Warszawa 2015.
- Sławińska-Żak E.: Słownik komputerowy. Wydawnictwo Videograf II, Katowice 2003.
- Stallings W.: Systemy operacyjne. Robomatic, Wrocław 2004.
- Stallings W., Brown L.: Bezpieczeństwo systemów informatycznych. Zasady i praktyka. Helion, Gliwice 2019.
- Wilhelm T.: Profesjonalne testy penetracyjne. Helion, Gliwice 2014.
- Wołowski F., Zawiła-Niedźwiedzki J.: Bezpieczeństwo systemów informacyjnych. Edu/Libri, 2015.
- Wróblewski P.: Algorytmy. Struktury danych i techniki programowania. Helion, Gliwice 2015.

Zasoby internetowe [dostęp: 31.03.2019]:

- Barometr zawodów 2019. Raport podsumowujący badania w Polsce: https://barometrzawodow.pl/userfiles/Barometr/2019/raport_ogolnopolski_pl.pdf
- Baza danych standardów kwalifikacji/kompetencji zawodowych i modułowych programów szkoleń: ftp://kwalifikacje.praca.gov.pl

- Blog o analizie biznesowej i systemowej IT: http://analizait.pl
- Chip: https://www.chip.pl
- Computerworld: https://www.computerworld.pl
- Inżynieria oprogramowania: http://zasoby.open.agh.edu.pl/~10sdczerner/page/wstep.html
- Katalog znanych zagrożeń bezpieczeństwa: https://cve.mitre.org
- Komputer Świat: http://www.komputerswiat.pl
- Konferencja poświęcona rozwojowi świata hakerów: https://www.defcon.org
- Niezależne źródło informacji o bezpieczeństwie IT: https://zaufanatrzeciastrona.pl
- PC Format: https://www.pcformat.pl
- PC World: https://www.pcworld.pl
- Portal Asystent BHP: https://asystentbhp.pl
- Portal o tematyce archiwizacji danych: https://www.backupacademy.pl
- Portal o tematyce IT: https://idg.pl
- Portal poświęcony trendom bezpieczeństwa IT: https://hakin9.org
- Projekt Zintegrowany System Kwalifikacji: http://kwalifikacje.edu.pl
- Sektorowa Rama Kwalifikacji dla Sektora Informatycznego (SRK IT): http://kwalifikacje.edu.pl/sektorowa-rama-kwalifikacji-dla-sektora-informatycznego
- Serwisy i blogi powiązane z tematyką IT i programowania: https://polskifrontend.pl
- Standardy orzecznictwa lekarskiego ZUS: http://www.zus.pl/lekarze/publikacje/standardy-orzecznictwa-lekarskiego-zus
- Wyszukiwarka opisów zawodów: http://psz.praca.gov.pl/rynek-pracy/bazy-danych/klasyfikacja-zawodow-i-specjalnosci/wyszukiwarka-opisow-zawodow
- Zespół reagowania na incydenty bezpieczeństwa: https://www.cert.pl
- Zestawienie aktualnych zagrożeń bezpieczeństwa: https://www.kb.cert.org/vuls

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.
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 umożliwiająca 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, cząstkowe, 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”.
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	**Agregacja**	Proces łączenia się elementów w całość.	https://sjp.pl/agregacja [dostęp: 31.03.2019]
2	**Aktywa informacyjne**	Wszystko, co ma wartość dla organizacji z uwagi na zawarte informacje.	http://www.ofbor.pl/images/pliki/pkjbi.pdf [dostęp: 31.03.2019]

3	**Architektura systemu**	Podstawowa organizacja systemu teleinformatycznego, jego części składowe oraz powiązania między nimi.	Definicja opracowana przez zespół ekspercki na podstawie: https://fizyka.umk.pl/~jacek/dydaktyka/inzynieria/2014L/NRybarczyk_DiagramyKomponentow.pdf [dostęp: 31.03.2019]
4	**Audytor**	Osoba prowadząca systematyczną i uporządkowaną ocenę procesów: zarządzania ryzykiem, kontroli, ładu organizacyjnego. Pomaga organizacji osiągnąć założone cele i optymalizować efekty realizacji procesów.	Definicja opracowana przez zespół ekspercki na podstawie: https://www.iia.org.pl/o-nas/definicja-aw [dostęp: 31.03.2019]
5	**Cyberatak**	Każdy rodzaj ofensywnego działania w internecie osób lub organizacji, którego celem mogą być systemy informatyczne, sieci komputerowe, komputery lub inne urządzenia osobiste, w tym również wyrządzenie w nich szkód.	Definicja opracowana przez zespół ekspercki na podstawie: https://sjp.pwn.pl/sjp/cyberatak;5606168.html [dostęp: 31.03.2019]
6	**Cyberbezpieczeństwo**	Możliwość bezpiecznego użytkowania komputerów i systemów komputerowych zapewnione poprzez skuteczną ochronę przed atakami elektronicznymi.	Definicja opracowana przez zespół ekspercki na podstawie: https://mfiles.pl/pl/index.php/Cyberbezpiecze%C5%84stwo [dostęp: 31.03.2019]
7	**Dostęp zdalny**	Możliwość korzystania z zasobów oraz wszystkich funkcji odległego komputera przy pomocy sieci komputerowej.	Definicja opracowana przez zespół ekspercki na podstawie: https://technet.microsoft.com/pl-pl/library/dn629457(v=ws.11).aspx [dostęp: 31.03.2019]
8	**Implementacja**	Proces realizacji technicznej specyfikacji w postaci reguły, algorytmu lub programu.	Definicja opracowana przez zespół ekspercki na podstawie: http://definicja.net/co-to-jest-Implementacja [dostęp: 31.03.2019]
9	**Incydent**	Pojedyncze zdarzenie lub seria zdarzeń, związanych z bezpieczeństwem informacji niejawnych, które zagrażają ich poufności, dostępności lub integralności.	Definicja opracowana przez zespół ekspercki na podstawie: https://ochrona-niejawnych.pl/kiedy-mamy-do-czynienia-z-incydentem-bezpieczenstwa-teleinformatycznego [dostęp: 31.03.2019]
10	**Log**	Zapis historii działania systemu komputerowego.	Definicja opracowana przez zespół ekspercki na podstawie: https://sjp.pwn.pl/sjp/log-l;2566265.html [dostęp: 31.03.2019]
11	**Oprogramowanie antywirusowe**	Program komputerowy wykrywający i likwidujący programy dezorganizujące pracę systemu komputerowego (wirusy).	Definicja opracowana przez zespół ekspercki na podstawie: https://sjp.pwn.pl/sjp/antywirusowy;2440843.html [dostęp: 31.03.2019]
12	**Oprogramowanie narzędziowe**	Zbiór programów komputerowych, służących do analizowania działania systemu operacyjnego komputera i jego zasobów, wykrywania ewentualnych nieprawidłowości, ich usuwania oraz optymalizowania pracy systemu komputerowego.	Definicja opracowana przez zespół ekspercki na podstawie: Sławińska-Żak E.: Słownik komputerowy. Wydawnictwo Videograf II, Katowice 2003

13	**Oprogramowanie systemowe**	Zespół programów umożliwiających sterowanie i zarządzanie zasobami komputera, tworzący warunki do rozwijania i wykonywania innych programów.	Definicja opracowana przez zespół ekspercki na podstawie: Stallings W.: Systemy operacyjne. Robomatic, Wrocław 2004
14	**Oprogramowanie użytkowe**	Zbiór programów wykorzystywanych bezpośrednio przez użytkownika w celu realizacji określonych zadań. Oprogramowanie użytkowe korzysta z systemu operacyjnego.	Definicja opracowana przez zespół ekspercki na podstawie: Stallings W.: Systemy operacyjne. Robomatic, Wrocław 2004
15	**Ryzyko**	Możliwość, że coś się nie uda; też: przedsięwzięcie, którego wynik jest niepewny.	https://sjp.pwn.pl/slowniki/ryzyko.html [dostęp: 31.10.2019]
16	**Serwer**	Komputer lub program przeznaczony do obsługi użytkowników przez udostępnianie ich komputerom swoich zasobów i wykonywanie otrzymanych poleceń.	https://sjp.pwn.pl/sjp/serwer;2575297.html [dostęp: 31.03.2019]
17	**Serwerownia**	Pomieszczenie, w którym znajdują się i działają serwery.	Definicja opracowana przez zespół ekspercki na podstawie: https://www.computerworld.pl/news/Czym-rozni-sie-serwerownia-od-centrum-danych,369934.html [dostęp: 31.03.2019]
18	**Stacja robocza**	Wydajny komputer, który został zaprojektowany pod kątem określonych zastosowań.	https://www.pcworld.pl/news/Stacjonarne-stacje-robocze,404287.html [dostęp: 31.03.2019]
19	**System teleinformatyczny**	Całość powiązanych ze sobą elementów, służąca przetwarzaniu danych na drodze elektronicznej.	Definicja opracowana przez zespół ekspercki na podstawie: http://www.serwisprawa.pl/definicje,322,system-teleinformatyczny [dostęp: 31.03.2019]
20	**System wykrywania i zapobiegania naruszeniom**	Technologie wdrażane w fizycznych urządzeniach sieciowych wykorzystywane do wykrywania włamań (ang. Intrusion Detection System, IDS) oraz im zapobiegania (ang. Intrusion Prevention System, IPS).	Definicja opracowana przez zespół ekspercki na podstawie: https://repozytorium.ukw.edu.pl/bitstream/handle/item/3532/Ids%20Ips%20systemy%20wykrywania%20i%20zapobiegania%20wlamaniom%20do%20sieci%20komputerowych.pdf?sequence=1&isAllowed=y [dostęp: 31.03.2019]
21	**Urządzenie końcowe**	Urządzenie telekomunikacyjne przeznaczone do podłączenia bezpośrednio lub pośrednio do zakończeń sieci.	Ustawa z dnia 16 lipca 2004 r. Prawo telekomunikacyjne http://prawo.sejm.gov.pl/isap.nsf/download.xsp/WDU20180001954/O/D20181954.pdf [dostęp: 31.03.2019]

www.psz.praca.gov.pl

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.

ISBN 978-83-7789-495-8 [183]