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 oprogramowania

(252901)



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 oprogramowania

(252901)

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 oprogramowania (252901)

© 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 [182]

Publikacja bezpłatna

Zdjęcie na okładce (źródło): https://foter.com/photo/woman-working-on-computer-contemplating-in-office [dostęp: 10.07.2018].

Wydawnictwo Naukowe Instytutu Technologii Eksploatacji – PIB
26-600 Radom, ul. K. Pułaskiego 6/10, tel. centr. (048) 364-42-41, fax (048) 364-47-65
e-mail: instytut@itee.radom.pl http://www.itee.radom.pl

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 ... 8
3. ZADANIA ZAWODOWE I WYMAGANE KOMPETENCJE ... 9
3.1. Zadania zawodowe ... 9
3.2. Kompetencja zawodowa Kz1: Analizowanie środowiska IT w celu identyfikacji zagrożeń i zapewnienia bezpieczeństwa oprogramowania ... 9
3.3. Kompetencja zawodowa Kz2: Monitorowanie oprogramowania, raportowanie i analizowanie zagrożeń ... 10
3.4. Kompetencje społeczne ... 11
3.5. Profil kompetencji kluczowych dla zawodu ... 12
3.6. Powiązanie kompetencji zawodowych z opisami poziomów Polskiej Ramy Kwalifikacji oraz Sektorowej Ramy Kwalifikacji ... 12
4. ODNIESIENIE DO SYTUACJI ZAWODU NA RYNKU PRACY I MOŻLIWOŚCI DOSKONALENIA ZAWODOWEGO ... 13
4.1. Możliwości podjęcia pracy w zawodzie ... 13
4.2. Instytucje oferujące kształcenie, szkolenie i/lub potwierdzanie kompetencji w ramach zawodu ... 14
4.3. Zarobki osób wykonujących dany zawód/daną grupę zawodów ... 14
4.4. Możliwości zatrudnienia osób niepełnosprawnych w zawodzie ... 15
5. ODNIESIENIE DO EUROPEJSKIEJ KLASYFIKACJI UMIEJĘTNOŚCI/KOMPETENCJI, KWALIFIKACJI I ZAWODÓW (ESCO) ... 16
6. ŹRÓDŁA DODATKOWYCH INFORMACJI O ZAWODZIE ... 16
7. SŁOWNIK POJĘĆ ... 17
7.1. Definicje powiązane z opisem informacji o zawodzie (zawodoznawcze) ... 17
7.2. Definicje związane z wykonywaniem zawodu (branżowe) ... 20

1. DANE IDENTYFIKACYJNE ZAWODU

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

Specjalista bezpieczeństwa oprogramowania 252901

1.2. Nazwy zwyczajowe zawodu

- Nie zidentyfikowano.

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), źródeł internetowych oraz wyników badań i analiz prowadzonych w projekcie PO KL (2011–2013) „Rozwijanie zbioru krajowych standardów kompetencji zawodowych wymaganych przez pracodawców”,
- analizy opisu zawodu zamieszczonego w wyszukiwarce opisów zawodów na Wortalu Publicznych Służb Zatrudnienia,
- zebranych opinii od recenzentów, członków panelu ewaluacyjnego oraz zespołu ds. walidacji i jakości informacji o zawodach.

Autorzy i eksperci opiniujący

Zespół Ekspercki:

- Bożena Tomczyńska-Dąbek – Centrum Informatyki Statystycznej, Warszawa.
- Krzysztof Trela – TISKO Krzysztof Trela, Ostrowiec Świętokrzyski.
- Wojciech Oparcik – Instytut Technologii Eksploatacji – PIB, Radom.

Zespół ds. walidacji i jakości informacji o zawodzie:

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

Recenzenci:

- Piotr Golonko – neoWEB Piotr Golonko, Białystok.
- Waldemar Grądzki – Uniwersyteckie Centrum Obliczeniowe Uniwersytet w Białymstoku.

Panel ewaluacyjny – przedstawiciele partnerów społecznych:

- Grażyna Mrozińska-Hotloś – Akademia Cisco, Lublin.
- Marek Mieńkowski – Stowarzyszenie Siła w Innowacji, Radom.

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 bezpieczeństwa oprogramowania identyfikuje zagrożenia dla systemów informatycznych, ustala, wdraża, aktualizuje procedury zapewniające bezpieczeństwo oprogramowania w organizacji.

2.2. Opis pracy i sposobu jej wykonywania

Opis pracy

Specjalista bezpieczeństwa oprogramowania odpowiada za bezpieczeństwo działania oprogramowania wykorzystywanego w firmie lub instytucji. Analizuje pod kątem bezpieczeństwa IT architekturę, infrastrukturę systemów informatycznych organizacji, realizowane przez nią procesy. Identyfikuje ryzyka i zagrożenia, przeciwdziała skutkom incydentów bezpieczeństwa[5] w użytkowanym oprogramowaniu, rekomenduje działania naprawcze. Definiuje i wdraża procedury usuwające zagrożenia i podnoszące poziom bezpieczeństwa oprogramowania. Wykonuje testy bezpieczeństwa zarówno dla tworzonych, jak i eksploatowanych systemów. W zakresie zapewnienia bezpieczeństwa oprogramowania współpracuje z:

- administratorem sieci,
- administratorem systemów operacyjnych,
- administratorem systemów bazodanowych,
- administratorami aplikacji,
- inspektorem ochrony danych (IOD),
- innymi specjalistami technologii informatycznych, zatrudnionymi w organizacji.

WAŻNE:
Pracę w zawodzie **specjalista bezpieczeństwa oprogramowania** może wykonywać osoba posiadająca doświadczenie zawodowe zdobyte wcześniej w jednym z obszarów: administrowania systemami, zarządzania bezpieczeństwem IT, analizy ryzyka, audytu systemów informatycznych.

Sposoby wykonywania pracy

Specjalista bezpieczeństwa oprogramowania w trakcie wykonywania pracy:

- zapoznaje się z dokumentacją techniczną systemów informatycznych, wykorzystywanych w firmie,
- sprawdza zgodność systemów informatycznych ze standardami bezpieczeństwa,
- definiuje zasady tworzenia oprogramowania w zakresie bezpieczeństwa,
- analizuje środowisko informatyczne w celu wykrycia zagrożeń,
- identyfikuje ryzyka i zagrożenia w zakresie bezpieczeństwa oprogramowania,
- dba o wysoki poziom bezpieczeństwa tworzonego i wdrożonego oprogramowania,
- monitoruje środowisko informatyczne w organizacji,
- eliminuje luki[6] i podatności[8] oprogramowania,
- realizuje testy penetracyjne[10] w zakresie oprogramowania,
- definiuje i wdraża procedury zapewniające oczekiwany poziom bezpieczeństwa,
- wykonuje testy bezpieczeństwa zarówno dla tworzonych, jak i eksploatowanych systemów informatycznych,
- sprawdza wydajność wykorzystywanych programów,
- bierze udział w audytach[1] i kontrolach bezpieczeństwa systemów informatycznych,

- instaluje i konfiguruje różnego rodzaju programy narzędziowe[9] do wykrywania zagrożeń, kontrolowania poprawności działania systemów informatycznych,
- sprawdza wydajność wykorzystywanych programów,
- projektuje i sporządza raporty zagrożeń.

WAŻNE:
W pracy **specjalisty bezpieczeństwa oprogramowania** niezbędna jest znajomość regulacji i norm z zakresu bezpieczeństwa teleinformatycznego i ochrony informacji.

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

Specjalista bezpieczeństwa oprogramowania pracuje zwykle w dobrze oświetlonym, klimatyzowanym pomieszczeniu biurowym, laboratorium komputerowym. Możliwe jest także wykonywanie pracy poza siedzibą pracodawcy, np. w domu. Podstawowym narzędziem pracy specjalisty jest terminal/komputer podłączony do infrastruktury informatycznej organizacji, w której pracuje.

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

Wykorzystywane maszyny i narzędzia pracy

Specjalista bezpieczeństwa oprogramowania w swojej pracy korzysta ze zintegrowanego środowiska komputerowego (sprzęt, peryferia[7], system operacyjny), a także z:

- systemów monitorowania bezpieczeństwa informatycznego,
- systemów zarządzania zdarzeniami[13] oraz incydentami bezpieczeństwa,
- norm i standardów dotyczących bezpieczeństwa oprogramowania,
- narzędzi do przeprowadzania testów służących wykryciu luk i podatności oprogramowania na różnego rodzaju ataki,
- narzędzi do analizy złośliwego oprogramowania[14],
- oprogramowania biurowego.

Organizacja pracy

Praca **specjalisty bezpieczeństwa oprogramowania**, zależnie od firmy, może odbywać się w stałych godzinach pracy w dni robocze lub w systemie zmianowym, także w niedziele i dni świąteczne. Wykonując swoje zadania, wykorzystuje specjalistyczne oprogramowanie. W sytuacjach awaryjnych od specjalisty wymaga się większej dyspozycyjności, wydłużonego czasu pracy. Może być także zobligowany do pełnienia dyżuru telefonicznego albo wykonywania pewnych zadań, łącząc się z domu z siecią firmy. Specjalista jest w pełni samodzielny, działa często w sytuacjach problemowych, pod presją czasu i przełożonych, ponosi odpowiedzialność i ryzyko wynikające z podejmowanych decyzji i działań. Praca specjalisty bezpieczeństwa oprogramowania ma charakter indywidualny i wymaga ciągłego dokształcania, podnoszenia kwalifikacji i śledzenia zmian na rynku bezpieczeństwa informatycznego.

WAŻNE:
Praca **specjalista bezpieczeństwa oprogramowania** wymaga bardzo dużego zaangażowania, silnej motywacji do pracy oraz dążenia do rozwoju zawodowego. Bardzo ważna jest umiejętność pracy w stresie i pod presją czasu.

Zagrożenia mające wpływ na bezpieczeństwo pracy człowieka

Osoba pracująca jako **specjalista bezpieczeństwa oprogramowania** narażona jest na:

- przeciążenia układu kostno-stawowego z powodu wymuszonej pozycji ciała podczas długotrwałej pracy przy komputerze, powodujące:
  - zmiany zwyrodnieniowe kręgosłupa,
  - wady postawy,
  - zmiany w układzie kostno-stawowym nadgarstka;
- przeciążenia narządu wzroku spowodowane intensywną i długotrwałą pracą przy komputerze, złe lub niewłaściwe sztuczne oświetlenie pomieszczeń, powodujące:
  - osłabienie wzroku,
  - ból, łzawienie oczu;
- obciążenia nerwowo-psychiczne spowodowane pracą pod presją czasu, przełożonych, koniecznością szybkiego podejmowania odpowiedzialnych decyzji, powodujące:
  - stres,
  - nerwicę,
  - depresję;
- podwyższony poziom hałasu podczas pracy w pomieszczeniu, w którym stoi wiele komputerów, drukarek;
- czynniki biologiczne przy słabej wentylacji pomieszczeń.

WAŻNE:
Szczególne ważne jest organizowanie stanowiska pracy zgodnie z przepisami dotyczącymi bezpieczeństwa i higieny pracy oraz zasadami ergonomii[4] stanowisk pracy.

2.4. Wymagania psychofizyczne i zdrowotne

Wymagania psychofizyczne

Dla pracownika wykonującego zawód **specjalista bezpieczeństwa oprogramowania** ważne są:

w kategorii wymagań fizycznych
- sprawność układu kostno-stawowego,
- sprawność układu mięśniowego,
- sprawność kończyn górnych,
- sprawność narządu wzroku,
- sprawność narządów słuchu;

w kategorii sprawności sensomotorycznych
- koordynacja wzrokowo-ruchowa,
- ostrość wzroku,
- ostrość słuchu,
- rozróżnianie barw,
- spostrzegawczość,
- zręczność rąk,
- zręczność palców;

w kategorii sprawności i zdolności
- uzdolnienia matematyczne,
- zdolność pracy w szybkim tempie,
- zdolność koncentracji uwagi,
- rozumowanie logiczne,
- wyobraźnia i myślenie twórcze,
- dobra pamięć,

- podzielność uwagi,
- zdolność do współdziałania,
- zdolność przekonywania,
- łatwość wypowiadania się w mowie i piśmie;

w kategorii cech osobowościowych
- samodzielność,
- samokontrola,
- zainteresowania informatyczne,
- rzetelność,
- dociekliwość,
- odporność na stres,
- cierpliwość,
- kreatywność,
- predyspozycje do długotrwałej pracy w pozycji siedzącej,
- łatwość przechodzenia z jednej czynności do drugiej,
- wytrzymałość na długotrwały wysiłek intelektualny,
- wytrwałość,
- dokładność,
- gotowość do ustawicznego uczenia się oraz dzielenia się wiedzą.

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

Wymagania zdrowotne

Praca **specjalisty bezpieczeństwa oprogramowania** powoduje duże obciążenie psychiczne i fizyczne. Osoba wykonująca ten zawód nie może być znerwicowana, leczyć się z powodu zaawansowanych chorób krążenia. Nie jest natomiast wymagana duża sprawność fizyczna. Specjalista bezpieczeństwa oprogramowania musi posiadać dobry wzrok oraz sprawność, umożliwiającą swobodne posługiwanie się komputerem.

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 podjęcia pracy w zawodzie **specjalista bezpieczeństwa oprogramowania** preferowane jest wykształcenie wyższe co najmniej I stopnia. Mogą to być m.in. studia na kierunkach: informatyka, elektronika, automatyka i robotyka, ekonometria, telekomunikacja oraz kierunkach pokrewnych.

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

Nie ma wymogów formalnych w zakresie niezbędnych kwalifikacji czy uprawnień, dopuszczających do wykonywania zawodu specjalista bezpieczeństwa oprogramowania.

Atutem przy zatrudnieniu **specjalisty bezpieczeństwa oprogramowania** są:
- udokumentowane doświadczenie na identycznym lub pokrewnym stanowisku pracy,

- certyfikaty potwierdzające znajomość języka angielskiego na różnych poziomach zaawansowania,
- posiadanie certyfikatów ukończeniu specjalistycznych kursów i szkoleń, potwierdzających wiedzę i umiejętności z zakresu bezpieczeństwa cybernetycznego[2], np.:
  - CISA (Certified Information Systems Auditor),
  - CompTIA Security,
  - GIAC Security Essential.

2.6. Możliwości rozwoju zawodowego, awansu i potwierdzania kompetencji

Możliwości rozwoju zawodowego i awansu

Specjalista bezpieczeństwa oprogramowania po zdobyciu niezbędnego doświadczenia może awansować na:
- starszego specjalistę bezpieczeństwa oprogramowania,
- eksperta do spraw bezpieczeństwa oprogramowania,
- kierownika działu odpowiadającego za bezpieczeństwo informatyczne w firmie.

Osoba pracująca w zawodzie **specjalista bezpieczeństwa oprogramowania** może podnosić swoje kompetencje poprzez:
- uczestnictwo w szkoleniach, warsztatach, konferencjach dotyczących zagadnień bezpieczeństwa systemów informatycznych,
- zdobywanie certyfikatów na szkoleniach specjalistycznych,

Możliwości rozwoju zawodowego stwarza również ukończenie studiów podyplomowych, związanych z bezpieczeństwem oprogramowania oraz podjęcie kształcenia/szkolenia w zawodach pokrewnych.

Możliwości potwierdzania kompetencji

Obecnie (2018 r.) w zawodzie **specjalista bezpieczeństwa oprogramowania** nie ma możliwości potwierdzania kompetencji zawodowych zarówno w edukacji formalnej, jak i pozaformalnej.

Formą poświadczenia kompetencji w zawodzie **specjalista bezpieczeństwa oprogramowania** jest zdobywanie certyfikatów potwierdzających posiadanie wiedzy i umiejętności, np.:
- CISSP (Certified Information Systems Security Professional),
- CISM (Certified Information Security Manager),
- CRISC (Certified in Risk and Information Systems Control),
- CEH (Certified Ethical Hacker),
- OSCE (Offensive Security Certified Expert),
- OSWE (Offensive Security Web Expert),
- OSCP (Offensive Security Certified Professional),
- GIAC Certified Web Application Defender,
- GIAC Web Application Penetration Tester.

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 oprogramowania** może rozszerzać swoje kompetencje zawodowe w zawodach pokrewnych:

Nazwa zawodu pokrewnego zgodnie z Klasyfikacją zawodów i specjalności	Kod zawodu
Specjalista bezpieczeństwa systemów teleinformatycznych	252902
Specjalista do spraw systemów zarządzania bezpieczeństwem informacji	252903

3. ZADANIA ZAWODOWE I WYMAGANE KOMPETENCJE

3.1. Zadania zawodowe

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

Z1 Analizowanie środowiska informatycznego pod kątem identyfikacji zagrożeń bezpieczeństwa oprogramowania.
Z2 Opracowywanie procedur usuwających zagrożenia i podnoszących poziom bezpieczeństwa oprogramowania.
Z3 Wdrażanie procedur bezpieczeństwa oprogramowania.
Z4 Monitorowanie oprogramowania w celu wykrycia zagrożeń.
Z5 Raportowanie i analizowanie zagrożeń.
Z6 Wykonywanie testów oraz audytów bezpieczeństwa aplikacji, systemów informatycznych oraz infrastruktury IT.

3.2. Kompetencja zawodowa Kz1: Analizowanie środowiska IT w celu identyfikacji zagrożeń i zapewnienia bezpieczeństwa oprogramowania

Kompetencja zawodowa Kz1: Analizowanie środowiska IT w celu identyfikacji zagrożeń i zapewnienia bezpieczeństwa oprogramowania obejmuje zestaw zadań zawodowych Z1, Z2, Z3, do realizacji których wymagane są odpowiednie zbiory wiedzy i umiejętności.

Z1 Analizowanie środowiska informatycznego pod kątem identyfikacji zagrożeń bezpieczeństwa oprogramowania	
WIEDZA – zna i rozumie:	**UMIEJĘTNOŚCI – potrafi:**
• Normy międzynarodowe i krajowe oraz standardy określające zasady polityki bezpieczeństwa informatycznego; • Standardy zarządzania bezpieczeństwem oprogramowania; • Zagrożenia bezpieczeństwa oprogramowania; • Narzędzia do zapewnienia bezpieczeństwa IT; • Mechanizmy powstawania luk w oprogramowaniu ; • Systemy szyfrowania danych; • Systemy uwierzytelniania i kontroli dostępu; • Systemy wykrywania luk i podatności oprogramowania; • Systemy typu WAF (Web Application Firewall[11]); • Zagadnienia związane z bezpieczeństwem systemów operacyjnych, usług sieciowych i baz danych.	• Stosować międzynarodowe i krajowe normy i standardy polityki bezpieczeństwa; • Określać bezpieczne warunki pracy oprogramowania; • Identyfikować zagrożenia bezpieczeństwa oprogramowania; • Analizować ryzyka związane z bezpieczeństwem IT; • Definiować/opiniować specyficzne wymagania z zakresu bezpieczeństwa IT; • Definiować zasady uwierzytelniania[12] i kontroli dostępu; • Rekomendować rozwiązania w zakresie bezpieczeństwa IT.

Z2 Opracowywanie procedur usuwających zagrożenia i podnoszących poziom bezpieczeństwa oprogramowania	
WIEDZA – zna i rozumie:	**UMIEJĘTNOŚCI – potrafi:**
• Normy międzynarodowe i krajowe oraz standardy określające zasady polityki bezpieczeństwa informatycznego; • Standardy zarządzania bezpieczeństwem oprogramowania; • Procesy, systemy i techniki badania podatności oprogramowania; • Programy narzędziowe do zarządzania, monitorowania i dokumentowania zdarzeń bezpieczeństwa; • Narzędzia wykorzystywane do zapewnienia bezpieczeństwa IT; • Zagadnienia związane z bezpieczeństwem baz danych, systemów operacyjnych, sieci.	• Stosować międzynarodowe i krajowe normy i standardy polityki bezpieczeństwa IT w definiowanych procedurach bezpieczeństwa; • Określać bezpieczne warunki pracy oprogramowania w definiowanych procedurach bezpieczeństwa; • Wykorzystywać programy narzędziowe do zarządzania, monitorowania i dokumentowania zdarzeń bezpieczeństwa; • Stosować systemy wykrywania luk i podatności oprogramowania; • Opracowywać procedury mające na celu zapewnienie oczekiwanego poziomu bezpieczeństwa oprogramowania.

Z3 Wdrażanie procedur bezpieczeństwa oprogramowania	
WIEDZA – zna i rozumie:	**UMIEJĘTNOŚCI – potrafi:**
• Procedury bezpieczeństwa; • Zasady wdrażania procedur bezpieczeństwa oprogramowania; • Narzędzia do wykrywania zdarzeń i incydentów bezpieczeństwa; • Narzędzia poprawiające poziom bezpieczeństwa IT; • Zagadnienia związane z bezpieczeństwem baz danych, systemów operacyjnych, sieci.	• Instalować narzędzia do wykrywania zdarzeń i incydentów bezpieczeństwa i konfigurować zgodnie z zaleceniami procedur bezpieczeństwa oprogramowania; • Instalować narzędzia do zapewnienia bezpieczeństwa IT i konfigurować zgodnie z zaleceniami procedur bezpieczeństwa oprogramowania; • Współpracować z innymi specjalistami IT w zakresie wdrażania procedur bezpieczeństwa.

3.3. Kompetencja zawodowa Kz2: Monitorowanie oprogramowania, raportowanie i analizowanie zagrożeń

Kompetencja zawodowa Kz2: Monitorowanie oprogramowania, raportowanie i analizowanie zagrożeń obejmuje zestaw zadań zawodowych Z4, Z5, Z6, do realizacji których wymagane są odpowiednie zbiory wiedzy i umiejętności.

Z4 Monitorowanie oprogramowania w celu wykrycia zagrożeń	
WIEDZA – zna i rozumie:	**UMIEJĘTNOŚCI – potrafi:**
• Narzędzia monitorujące systemy informatyczne; • Zagrożenia bezpieczeństwa systemów IT; • Metody usuwania wykrytych przypadków naruszenia bezpieczeństwa systemów informatycznych; • Parametry pracy systemów informatycznych; • Programy z grupy EPP (Endpoint Protection Platforms[3]); • Systemy wykrywania luk i podatności	• Instalować i konfigurować programy narzędziowe do kontrolowania parametrów pracy systemów informatycznych, monitorowania i zarządzania zdarzeniami oraz incydentami bezpieczeństwa; • Identyfikować i analizować zagrożenia związane z bezpieczeństwem systemów IT; • Izolować i usuwać zagrożenia bezpieczeństwa oprogramowania;

oprogramowania; • Dzienniki zdarzeń, logi funkcjonujące w systemach informatycznych.	• Analizować dzienniki zdarzeń, logi zdefiniowane w systemach informatycznych, narzędziach monitorujących; • Wdrażać i monitorować poprawki podnoszące poziom bezpieczeństwa oprogramowania.

Z5 Raportowanie i analizowanie zagrożeń	
WIEDZA – zna i rozumie:	**UMIEJĘTNOŚCI – potrafi:**
• Narzędzia monitorujące systemy informatyczne; • Techniki zbierania, precyzowania i weryfikacji informacji o stanie bezpieczeństwa oprogramowania; • Metody raportowania wykrytych przypadków naruszenia bezpieczeństwa systemów informatycznych; • Zasady utrzymania bezpieczeństwa oprogramowania.	• Stosować narzędzia monitorujące do kontrolowania parametrów pracy systemów informatycznych, wykrywania zagrożeń; • Opracowywać raporty umożliwiające analizę monitorowanych incydentów; • Wykrywać zagrożenia bezpieczeństwa oprogramowania; • Rekomendować poprawki podnoszące poziom bezpieczeństwa oprogramowania.

Z6 Wykonywanie testów oraz audytów bezpieczeństwa aplikacji, systemów informatycznych oraz infrastruktury IT	
WIEDZA – zna i rozumie:	**UMIEJĘTNOŚCI – potrafi:**
• Normy międzynarodowe i krajowe oraz standardy określające zasady polityki bezpieczeństwa informatycznego; • Procedury bezpieczeństwa; • Ataki na aplikacje, systemy oraz infrastrukturę IT; • Techniki testów penetracyjnych; • Zasady definiowania celów i zakresów audytów zasobów środowiska informatycznego oraz procesów informatycznych; • Zasady przeprowadzania i analizy audytu zasobów środowiska informatycznego oraz procesów informatycznych; • Metody, techniki i narzędzia stosowane w audycie zasobów środowiska informatycznego oraz procesów informatycznych.	• Stosować międzynarodowe i krajowe normy i standardy polityki bezpieczeństwa IT; • Wykonywać testy bezpieczeństwa; • Projektować audyty zasobów środowiska informatycznego oraz procesów informatycznych; • Przeprowadzać i analizować audyty zasobów środowiska informatycznego oraz procesów informatycznych; • Wykorzystywać narzędzia stosowane na potrzeby przeprowadzenia audytu systemów IT.

3.4. Kompetencje społeczne

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

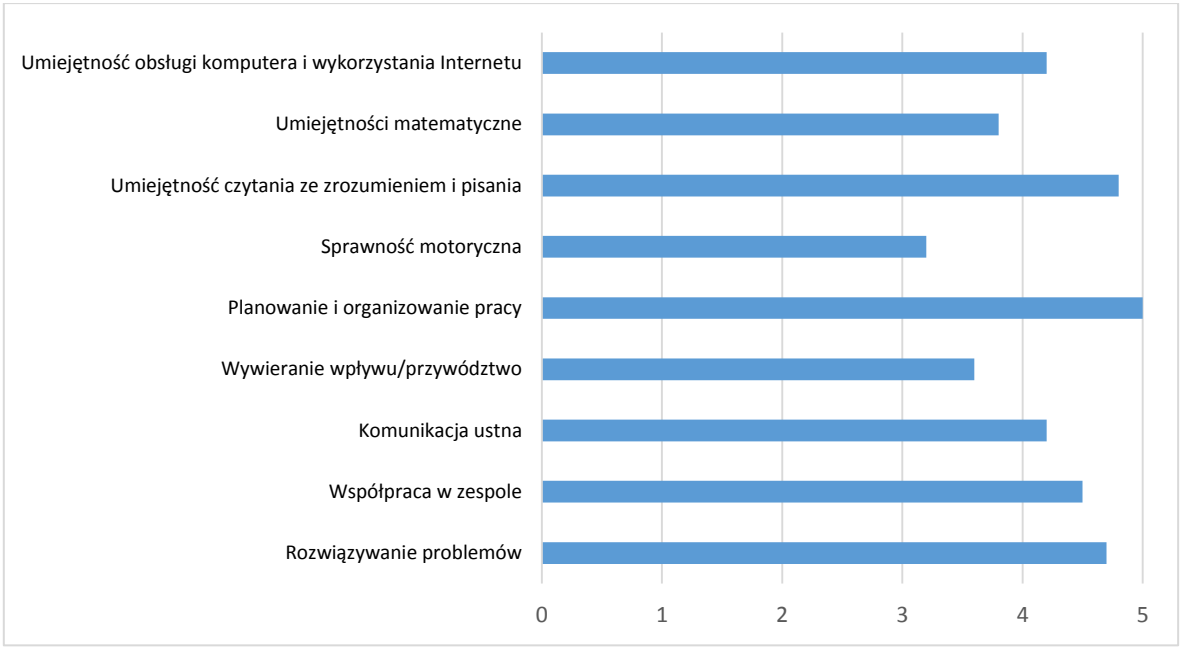
W szczególności pracownik jest gotów do:

- Ponoszenia odpowiedzialności za własne działania w zakresie zapewnienia bezpieczeństwa oprogramowania.
- Podejmowania samodzielnych decyzji mających wpływ na bezpieczeństwo oprogramowania w organizacji.
- Doskonalenia kompetencji zawodowych w sposób ustawiczny w celu doskonalenia jakości bezpieczeństwa oprogramowania.

- Oceniania działań własnych oraz osób, z którymi współpracuje, w zakresie zapewnienia bezpieczeństwa oprogramowania.
- Postępowania zgodnie z zasadami etyki zawodowej w branży IT.

3.5. Profil kompetencji kluczowych dla zawodu

Pracownik powinien posiadać 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 oprogramowania**.



Rys. 1. Profil kompetencji kluczowych dla zawodu **specjalista bezpieczeństwa oprogramowania**

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 oprogramowania** 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 oprogramowania może znaleźć zatrudnienie w:
- dużych korporacjach,
- przedsiębiorstwach dużej i średniej wielkości,
- firmach i centrach kompetencyjnych, specjalizujących się w usługach z zakresu bezpieczeństwa teleinformatycznego.

Największe zainteresowanie pracownikami w tym zawodzie wykazują następujące branże:
- bankowość, finanse i ubezpieczenia,
- telekomunikacja i zaawansowane technologie informatyczne,
- przemysł,
- handel i sprzedaż.

Widoczny jest znaczący deficyt tego typu specjalistów zarówno na rynku polskim, jak i europejskim. Spowodowane jest to rosnącym poziomem świadomości kadry zarządzającej w firmach w tym zakresie, jak i regulacjami prawnymi, narzucającymi na przedsiębiorców konkretne obowiązki w odniesieniu do przetwarzania danych.

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: 10.07.2018]**:**
Ranking (monitoring) zawodów deficytowych i nadwyżkowych:
http://mz.praca.gov.pl
https://www.mpips.gov.pl/analizy-i-raporty/raporty-sprawozdania/rynek-pracy/zawody-deficytowe-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 (2018 r.) w ramach formalnego systemu kształcenia nie przygotowuje się kandydatów do pracy w zawodzie **specjalista bezpieczeństwa oprogramowania.**

Kompetencje przydane do wykonywania tego zawodu można uzyskać i potwierdzić w ramach studiów I, II stopnia oraz studiów podyplomowych. Oferują je uczelnie techniczne, uniwersytety oraz wyższe szkoły zawodowe na wielu kierunkach i w specjalnościach, związanych z bezpieczeństwem oprogramowania.

Szkolenie

Szkolenia w zakresie bezpieczeństwa oprogramowania realizowane są przez firmy specjalizujące się w tym zakresie.

Szkolenia prowadzone przez firmy komercyjne z reguły kończą się egzaminem i wydaniem certyfikatu, który potwierdza uzyskaną przez uczestnika wiedzę i umiejętności, wynikające z oferty programowej danego szkolenia.

Inną formą nabywania wiedzy, umiejętności i doświadczenia w zawodzie **specjalista bezpieczeństwa oprogramowania** jest samokształcenie. Źródłami wiedzy w tym zakresie m.in. mogą być:
- portale specjalistyczne,
- blogi specjalistów bezpieczeństwa,
- webinaria i nagrania z konferencji tematycznych,
- kursy i szkolenia on-line z zakresu bezpieczeństwa w cyberprzestrzeni.

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: 10.07.2018]**:**

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

Szkolnictwo zawodowe:
https://www.gov.pl/web/edukacja/ksztalcenie-zawodowe
http://doradztwo.ore.edu.pl/wybieram-zawod
http://www.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

Obecnie (2018 r.) wynagrodzenie osób pracujących na stanowiskach właściwych dla zawodu **specjalista bezpieczeństwa oprogramowania** jest zróżnicowane i wynosi od 5000 zł do 17 000 zł miesięcznie brutto w przeliczeniu na jeden etat.

Poziom wynagrodzeń:
- w przypadku stanowisk o niższym poziomie wymagań i bez wymogu kilkuletniego doświadczenia zaczyna się od 5000 zł brutto,
- na stanowiskach wymagających wyższych kompetencji oraz znacznego doświadczenia (np. 3 lata) kształtuje się w przedziale od 7000 zł do 11 000 zł brutto,
- na stanowiskach kierowników bądź ekspertów mieści się w przedziale od 11 000 zł do 17 000 zł brutto.

Poziom wynagrodzeń osób wykonujących zawód specjalisty bezpieczeństwa oprogramowania uzależniony jest od:
- szczegółowego zakresu zadań i odpowiedzialności,
- doświadczenia w zawodzie oraz regionu Polski,
- rodzaju pracodawcy (prywatny, publiczny),
- branży, w której funkcjonuje pracodawca.

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: 10.07.2018]**:**
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-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 oprogramowania** możliwe jest zatrudnienie osób niepełnosprawnych.

Jest to uzależnione od stopnia niepełnosprawności. Przy zastosowaniu odpowiednich regulacji w zakresie czasu pracy oraz prawidłowej ergonomii stanowiska pracy dopuszczalne jest zatrudnienie w tym zawodzie osób:
- z niewielką dysfunkcją kończyn górnych (05-R), która nie wyklucza wykonywania 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,
- z dysfunkcją narządu wzroku (04-O), jeśli posiadana wada jest skorygowana odpowiednimi szkłami optycznymi lub soczewkami kontaktowymi, które zapewnią ostrość widzenia,

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: 30.06.2018 r.

- Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. poz. 1000).
- 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 20 kwietnia 2004 r. o promocji zatrudnienia i instytucjach rynku pracy (t.j. Dz. U. z 2018 r. poz. 1265 i 1149).
- Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. z 2017 r. poz. 1219, 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).

Literatura branżowa:

- Bilski T., Pankowski T., Stokłosa J.: Bezpieczeństwo danych w systemach informatycznych. PWN, Warszawa 2001.
- Luttgens J., Pepe M., Mandia K.: Incydenty bezpieczeństwa. Metody reagowania w informatyce śledczej. Helion, Gliwice 2016.
- Mandia K., Prosise Ch.: Hakerom śmierć! RM, Warszawa 2002.
- Wojciechowska-Filipek S., Ciekanowski Z.: Bezpieczeństwo funkcjonowania w cyberprzestrzeni jednostki organizacji państwa. CeDeWu Sp. z o.o., Warszawa 2016.

- Zalewski M.: Splątana sieć. Przewodnik po bezpieczeństwie nowoczesnych aplikacji WWW. Helion, Gliwice 2012.

Zasoby internetowe [dostęp: 10.07.2018]:

- Bankier.pl: https://www.bankier.pl/wiadomosc/Specjalisci-ds-bezpieczenstwa-IT-w-bankach-duze-zarobki-i-duze-wymagania-7515873.html
- Baza danych standardów kwalifikacji/kompetencji zawodowych i modułowych programów szkoleń: ftp://kwalifikacje.praca.gov.pl
- Benchmark: http://www.benchmark.pl/aktualnosci/praca-w-it-najlepsze-zawody-w-2018-roku.html
- Dziennik Internautów internet w życiu i biznesie: http://di.com.pl/eksperta-bezpieczenstwa-it-zatrudnie-od-zaraz-na-rynku-brakuje-specjalistow-ochrony-sieci-57070
- Forsal.pl: http://forsal.pl/artykuly/1098760,specjalista-ds-cyberbezpieczenstwa-praca-wynagrodzenie-zarobki-2018.htm
- Marketing biznes: https://marketingibiznes.pl/it/zawody-technologiczne
- The Open Web Application Security Project (OWASP): https://www.owasp.org
- PulsHR.pl: https://www.pulshr.pl/rekrutacja/praca-specjalista-ds-bezpieczenstwa-it-to-jeden-z-najbardziej-pozadanych-dzis-zawodow,37341.html
- Portal Asystent BHP: https://asystentbhp.pl
- Standardy orzecznictwa lekarskiego ZUS: http://www.zus.pl/lekarze/publikacje/standardy-orzecznictwa-lekarskiego-zus
- Sektorowa Rama Kwalifikacji dla Sektora Informatycznego (SRK IT): http://kwalifikacje.edu.pl/sektorowa-rama-kwalifikacji-dla-sektora-informatycznego
- Wynagrodzenia.pl Sedlak & Sedlak: https://wynagrodzenia.pl/moja-placa/ile-zarabia-specjalista-ds-bezpieczenstwa-informatycznego
- 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.
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	**Audyt bezpieczeństwa**	Audyt mający na celu weryfikację funkcjonowania rozwiązań technicznych i organizacyjnych mających zapewnić bezpieczeństwo komunikacji, danych, systemów i rządzeń teleinformatycznych, zgodności Platformy z obowiązującymi w tym zakresie przepisami prawa, obejmujący w szczególności audyt: zarządzania bezpieczeństwem informacji; bezpieczeństwa systemów informatycznych, zgodności z ustawą o ochronie danych osobowych; planów ciągłości działania; bezpieczeństwa aplikacji; legalności oprogramowania; testy penetracyjne, weryfikacja kodów źródłowych.	https://mc.bip.gov.pl/fobjects/download/299175/zal-1-slownik-pdf.html [dostęp: 10.07.2018]
2	**Bezpieczeństwo cybernetyczne – cyberbezpieczeństwo**	Definicja cyberbezpieczeństwa zależy od tego, do kogo się ona odnosi. Dla osób prywatnych może to być: ochrona prywatności, danych osobowych czy bezpieczeństwo zgromadzonych środków finansowych. Dla przedsiębiorstw cyberbezpieczeństwo to zapewnienie ciągłości funkcji biznesowych oraz ochrona poufnych danych i bezpieczeństwo zgromadzonych informacji. Dla państw oznacza to ochronę obywateli, państwowej infrastruktury teleinformatycznej przed atakiem czy naruszeniem integralności.	http://www.cyberobrona.pl [dostęp: 10.07.2018]
3	**Endpoint Protection Platforms**	Platforma ochrony punktów końcowych (EPP) to zestaw technologii i narzędzi programistycznych umożliwiających zabezpieczanie urządzeń końcowych. Jest to ujednolicone zapewnienia bezpieczeństwa, które łączy w sobie oprogramowanie antywirusowe, oprogramowanie antyszpiegowskie, wykrywanie włamań, zaporę sieciową i inne rozwiązania ochrony punktów końcowych.	https://www.techopedia.com/definition/30918/endpoint-protection-platform-epp [dostęp: 10.07.2018]
4	**Ergonomia**	Nauka o optymalnym przystosowaniu stanowisk, procesów i środowiska pracy do możliwości psychofizycznych człowieka, tak by nie tylko uchronić jego życie i zdrowie, lecz dać mu również możliwość jak najlepszego rozwoju osobowości.	https://encyklopedia.pwn.pl/szukaj/ergonomia.html [dostęp: 10.07.2018]
5	**Incydent bezpieczeństwa**	Naruszenie lub groźba naruszenia zasad bezpieczeństwa komputerowego, akceptowalnych zasad użytkowania lub standardowych praktyk zapewniania bezpieczeństwa.	https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf [dostęp: 10.07.2018]
6	**Luki oprogramowania**	Błędy oprogramowania wprowadzone na etapie jego specyfikacji, projektowania lub implementacji, z konfiguracją włącznie. Błędy te jednak nie powodują w normalnym trybie eksploatacji zaburzenia logiki funkcjonalności oprogramowania. Luki oprogramowania najczęściej uwidaczniają się na etapie eksploatacji.	http://rocznikikae.sgh.waw.pl/p/roczniki_kae_z45_15.pdf [dostęp: 10.07.2018]
7	**Peryferia**	Urządzenia niewchodzące w skład jednostki centralnej komputera, bezpośrednio przez nią sterowane, np. skaner, drukarka.	https://sjp.pl/peryferie [dostęp: 10.07.2018]
8	**Podatność oprogramowania**	Wykryte i zinwentaryzowane miejsce w kodzie lub konfiguracji oprogramowania, które można wykorzystać do przejęcia kontroli nad nim lub użyć niezgodnie z wolą jego właściciela lub użytkownika.	http://rocznikikae.sgh.waw.pl/p/roczniki_kae_z45_15.pdf [dostęp: 10.07.2018]

9	**Programy narzędziowe**	Program komputerowy, którego zadaniem w zależności od przeznaczenia jest wykonywanie zadań mających na celu analizowanie działania systemu operacyjnego komputera i jego zasobów, wykrywanie ewentualnych nieprawidłowości, ich usuwanie oraz optymalizacja pracy systemu.	http://www.edupedia.pl/words/index/show/509504_slownik_komputerowy-program_narzedziowy.html [dostęp: 10.07.2018]
10	**Test penetracyjny**	Proces pozwalający ocenić bieżący stan zabezpieczeń systemu. Test penetracyjny, popularnie nazywany pentestem, polega na identyfikacji, analizie i oszacowaniu ryzyka związanego z podatnościami i lukami zabezpieczeń.	https://shinsec.pl/test-penetracyjny [dostęp: 10.07.2018]
11	**Web Application Firewall**	Transparentny system ochrony aplikacji webowych. Dzięki prostemu modelowi działania pozwala na automatyczną kontrolę treści wchodzących do aplikacji (bez ingerencji użytkownika).	https://pomoc.home.pl/baza-wiedzy/czym-jest-waf-web-application-firewall [dostęp: 10.07.2018]
12	**Zasady uwierzytelniania**	Ma na celu upewnienie co najmniej jednej z dwóch stron biorących w nim udział o tożsamości drugiej. Jest identyfikacją w stopniu wystarczającym do przyznania odpowiednich uprawnień czy przywilejów osobie lub zidentyfikowanemu obiektowi. W uproszczeniu można powiedzieć, że jest to weryfikacja tożsamości przypisywanej osobom, stacjom lub źródłom danych.	https://www.computerworld.pl/news/Identyfikacja-uwierzytelnianie-i-autoryzacja,299422.html [dostęp: 10.07.2018]
13	**Zdarzenie bezpieczeństwa**	Jest to taki stan systemu, usługi lub sieci, który wskazuje na możliwe naruszenie polityki bezpieczeństwa informacji, błąd zabezpieczenia lub nieznaną dotychczas sytuację, która może być związana z bezpieczeństwem.	https://www.computerworld.pl/news/Zdarzenia-incydenty-i-zarzadzanie,323422.html [dostęp: 10.07.2018]
14	**Złośliwe oprogramowanie**	Termin „złośliwe oprogramowanie” odnosi się do oprogramowania lub aplikacji mobilnych zaprojektowanych specjalnie w celu zaszkodzenia użytkownikom lub uszkodzenia komputera, urządzenia mobilnego bądź zainstalowanych na nim aplikacji. Działanie złośliwego oprogramowania objawia się instalowaniem programów bez zgody użytkownika lub instalowaniem szkodliwych aplikacji takich jak wirusy.	https://support.google.com/webmasters/answer/3258249?hl=pl [dostęp: 10.07.2018]

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 [182]