ZINTEGROWANY SYSTEM KWALIFIKACJI

Sektorowa Rama Kwalifikacji jako narzędzie Zintegrowanego Systemu Kwalifikacji (ZSK) na przykładzie branży cyberbezpieczeństwa

dr Dawid Dymkowski

Warszawa, 30.10.2023 r.

Fundusze Europejskie Wiedza Edukacja Rozwój
Rzeczpospolita Polska
IBE kwalifikacje dla każdego
Unia Europejska Europejski Fundusz Społeczny

Od potrzeb rynku pracy do Sektorowych Ram Kwalifikacji

Edukacja a rynek pracy

niemal 4 na 5 pracodawców na świecie zgłasza trudności ze znalezieniem wykwalifikowanych pracowników

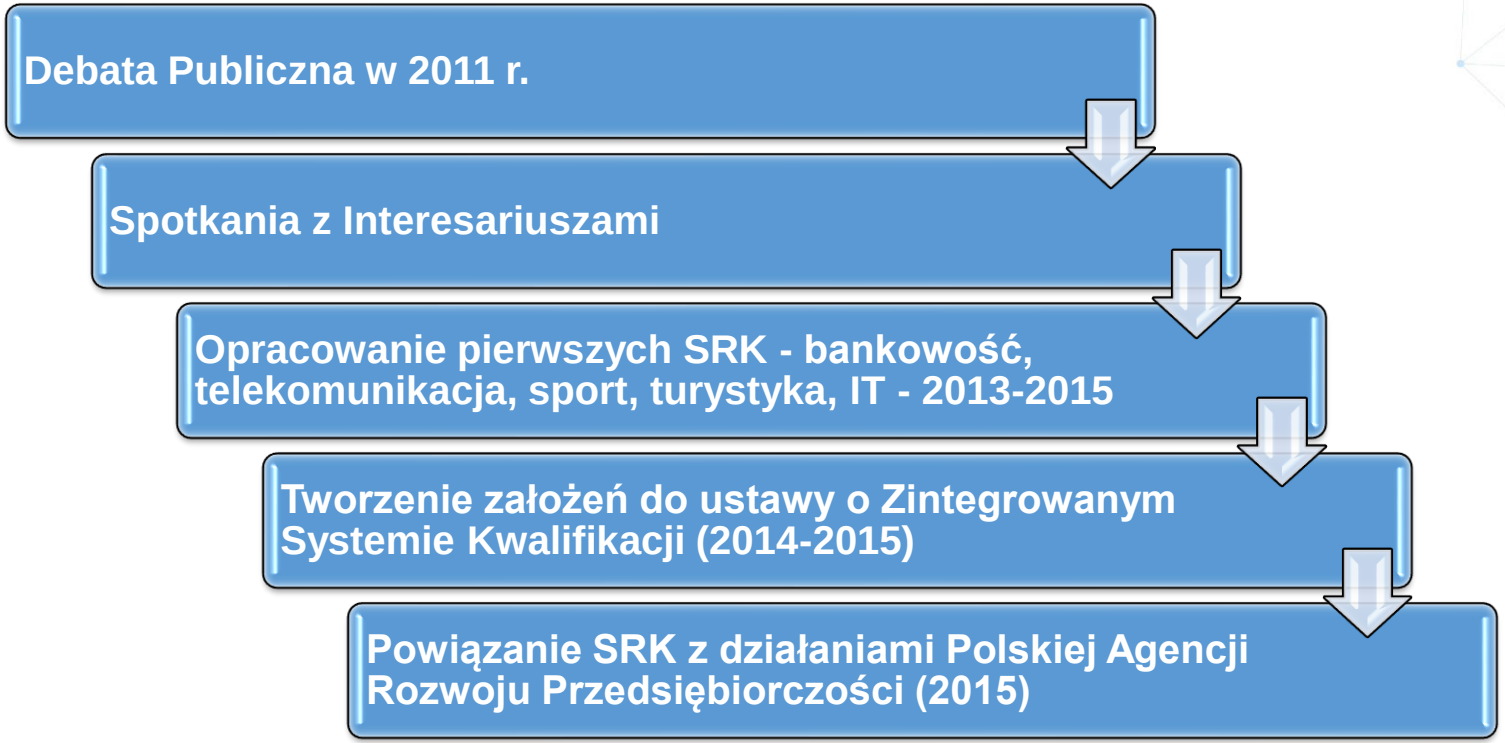
na świecie obserwowany jest widoczny rosnący trend dotyczący problemu z obsadzeniem wolnych stanowisk przez pracodawców

(2015 – 38% vs. 2023 – 77%)

w Polsce 72% pracodawców wskazuje problemy ze znalezieniem wykwalifikowanych pracowników

Źródło: ManpowerGroup, Global Talent Shortage 2023

Powstanie koncepcji Sektorowych Ram Kwalifikacji



Sektorowe Ramy Kwalifikacji

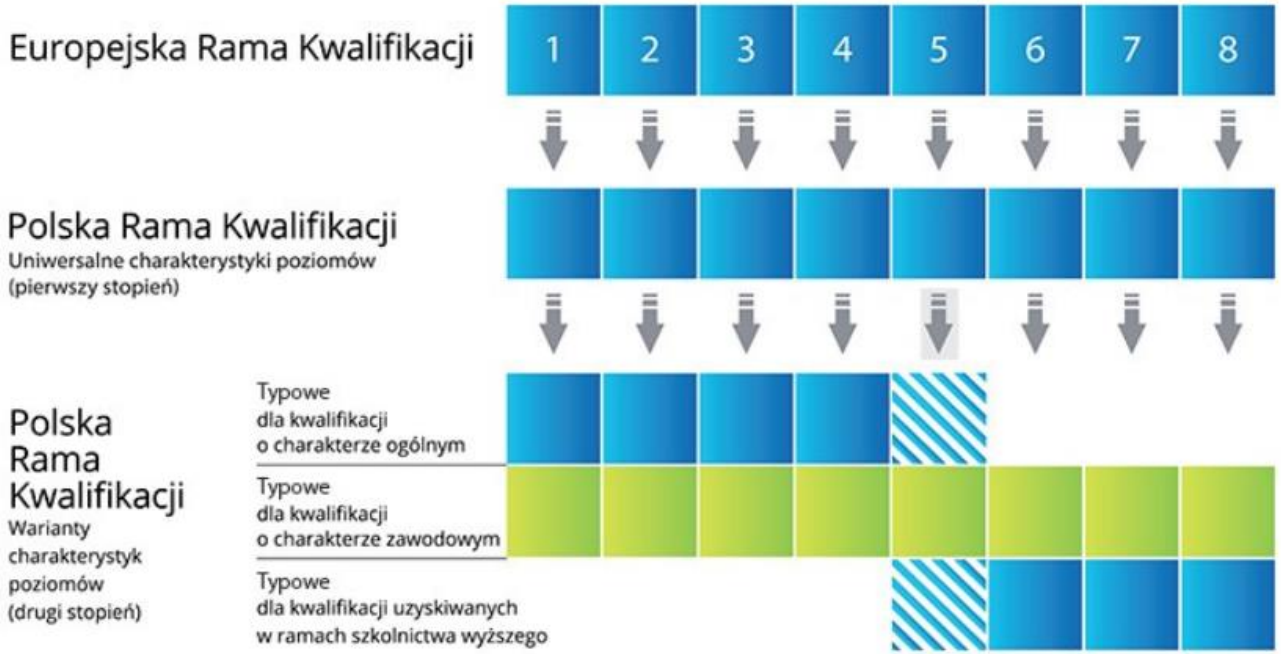
Opis poziomów kwalifikacji funkcjonujących w danym sektorze lub branży

21 opracowanych sektorowych ram kwalifikacji

6 sektorowych ram kwalifikacji włączonych do ZSK

7 sektorowych ram kwalifikacji w procesie włączana do ZSK

Budowa Polskiej Rama Kwalifikacji



Polska Rama Kwalifikacji, a Sektorowa Rama Kwalifikacji

Charakterystyka I stopnia PRK - uniwersalne

- (potrafi) wykonywać umiarkowanie złożone zadania bez instrukcji w zmiennych i nie w pełni przewidywalnych warunkach [P5U_U(1)]

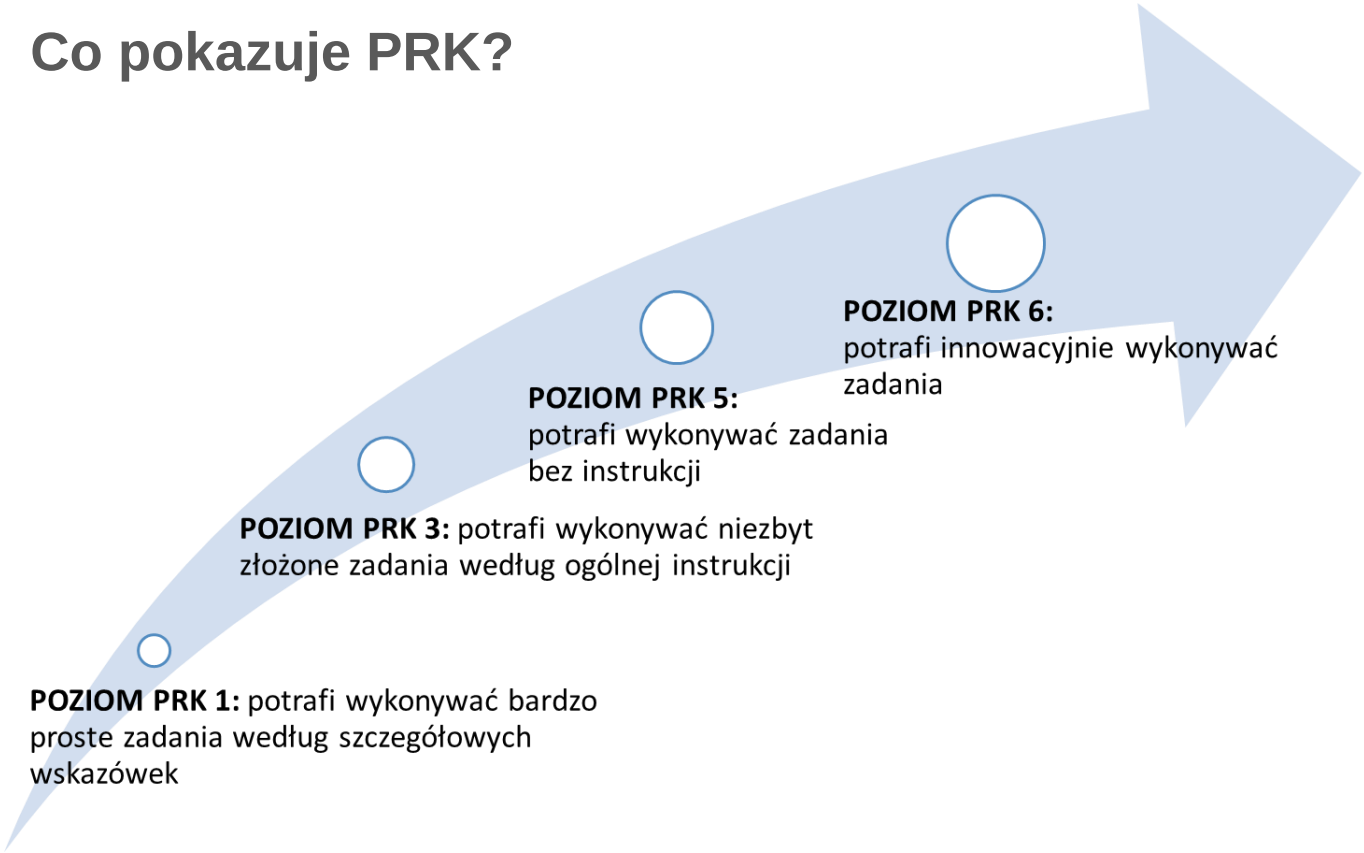
Charakterystyka II stopnia PRK - zawodowe

- (potrafi) analizować i oceniać przebieg oraz efekty działalności zawodowej, rozwiązywać nietypowe problemy i wprowadzać odpowiednie korekty [P5Z_UO(4)]

Charakterystyka SRK CYBER

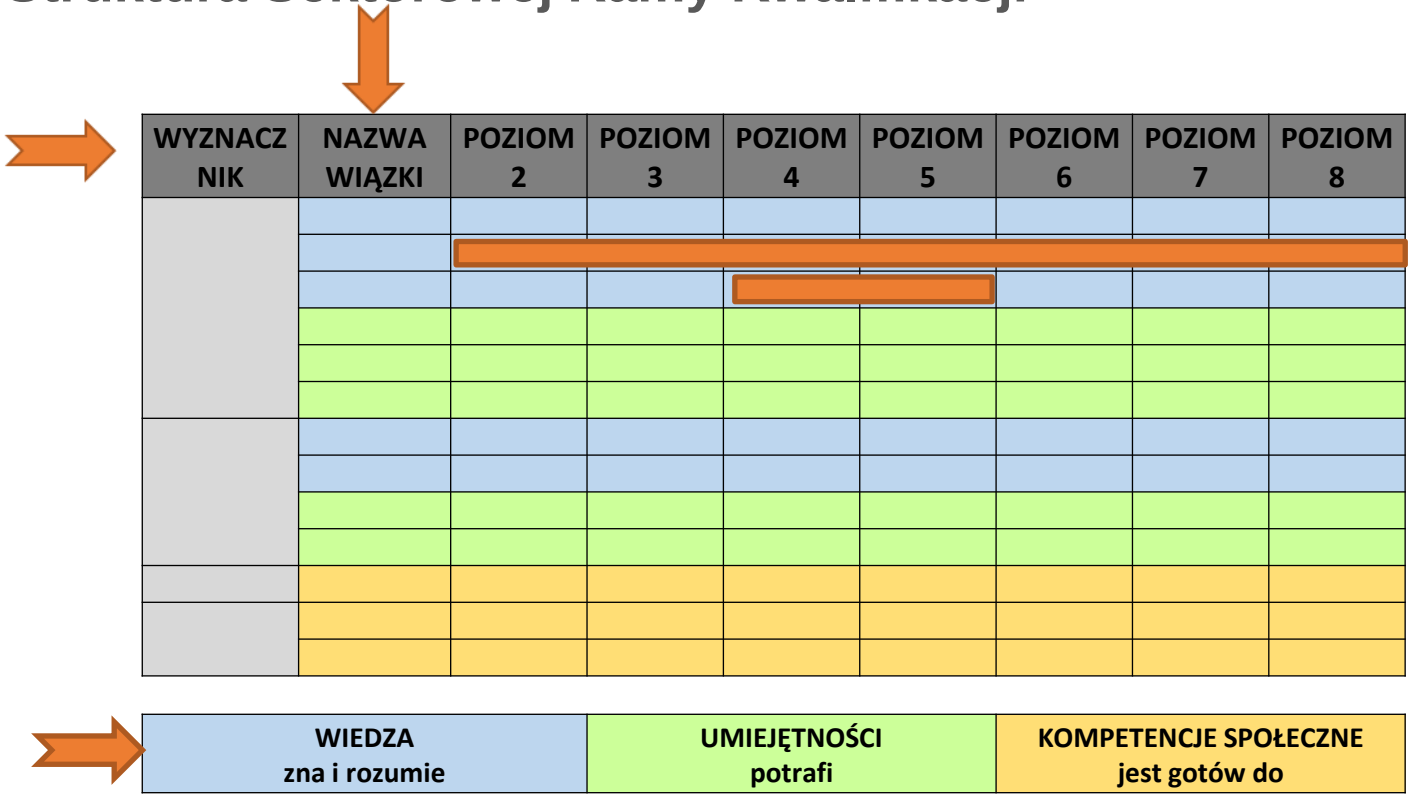
- (potrafi) analizować szkodliwe oprogramowanie oraz słabe punkty w systemach informatycznych

Co pokazuje PRK?



Budowa dotychczasowych SRK

Struktura Sektorowej Ramy Kwalifikacji

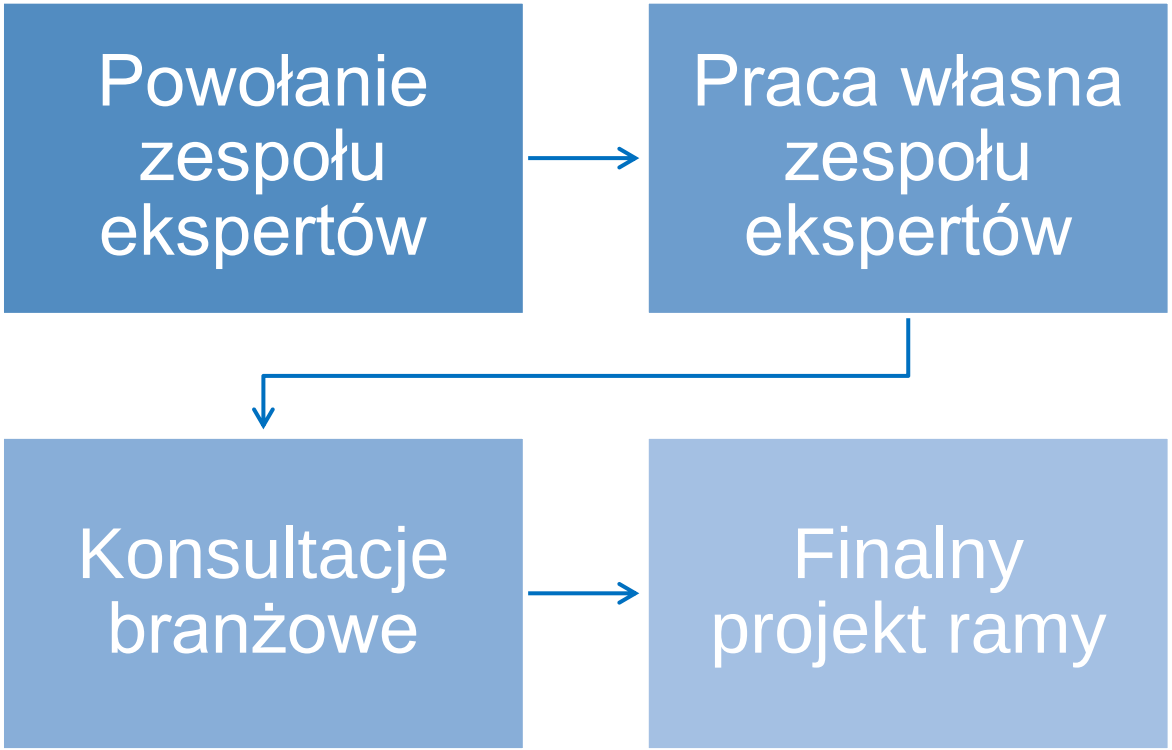


W jakim celu tworzone są SRK?

- ułatwienie rozpoczęcia ustrukturyzowanej dyskusji o potrzebach sektora dotyczących szeroko rozumianej edukacji
- odpowiedź na deregulację zawodów
- wsparcie na poziomie przedsiębiorstwa, w zarządzaniu zasobami ludzkimi czy zarządzaniu kompetencjami
- ułatwienie określania poziomów PRK dla kwalifikacji
- ułatwienie dopasowanie kompetencji posiadanych przez pracowników do potrzeb rynku pracy

Prace nad Sektorowymi Ramami Kwalifikacji

Proces tworzenia Sektorowych Ram Kwalifikacji



Zespoły eksperckie

- przedstawiciele istotnych i reprezentatywnych dla branży firm, instytucji, izb, organizacji, stowarzyszeń, itp.
- osoby reprezentujące różne poziomy firmowej/organizacyjnej hierarchii
- osoby reprezentujące wszystkie istotne dla sektora obszary działań zmierzających do wytwarzania produktów lub usług specyficznych dla danej branży
- osoby posiadające wiedzę na temat kompetencji kluczowych i specyficznych wykorzystywanych w pracy w danej branży
- osoby posiadające wiedzę na temat funkcjonujących i nadawanych w sektorze kwalifikacji
- przynajmniej jedna osoba posiadająca wiedzę na temat PRK i ZSK
- osoby przygotowane do pełnienia roli koordynatora projektu i moderatora pracy zespołu

ETAP I – określenie wyznaczników sektorowych oraz charakterystyk poziomów

Zdefiniowanie pojęć występujących w sektorze

Określenie głównych obszarów działalności sektora

Wskazanie kompetencji sektorowych

- Seminarium inaugurujące
- Praca warsztatowa
- Praca własna

ETAP II – konsultacje branżowe

- Badanie jakościowe z wykorzystaniem techniki IDI lub FGI
- Dodatkowe inicjatywy konsultacyjne zależne od branży

Minimum 100 osób

ETAP III – przygotowanie ostatecznej wersji ramy

Projekt SRK przygotowany przez ZE

FINALNY PROJEKT SEKTOROWEJ RAMY

Wnioski z konsultacji

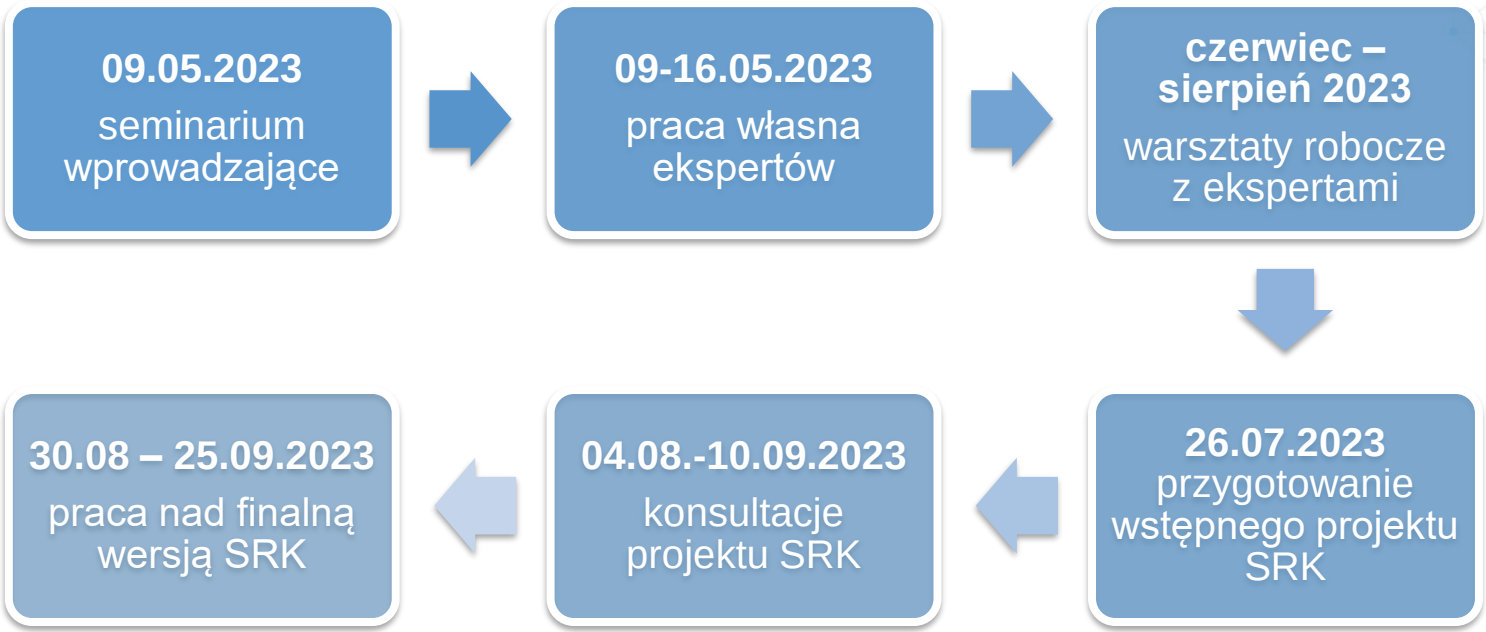
Sektorowa Rama Kwalifikacji w Cyberbezpieczeństwie

Zespół ekspertów Sektorowej Ramy Kwalifikacji CYBER

Kierownik zespołu ekspertów: **Beata Ostrowska**

W niniejszym postępowaniu zostanie wyłoniona część Zespołu Ekspertów licząca 9 przedstawicieli z obszaru cyberbezpieczeństwa:
Kategoria I Cyberbezpieczeństwo - 5 ekspertów
1.1. podkategoria I - bezpieczeństwo aplikacji/oprogramowania
1.2 podkategoria II - bezpieczeństwo danych
1.3 podkategoria III - bezpieczeństwo warstwy fizycznej
1.4. podkategoria IV - bezpieczeństwo połączeń
1.5 podkategoria V - bezpieczeństwo systemów organizacji
Kategoria II Informatyka Śledcza - 1 ekspert
Kategoria III Cyberbezpieczeństwo – edukacja pozaformalna – 1 ekspert
Kategoria IV Cyberbezpieczeństwo – edukacja formalna - 2 ekspertów
4.1. podkategoria I - szkolnictwo wyższe
4.2 podkategoria II - szkolnictwo branżowe

Prace nad Sektorową Ramą Kwalifikacji w Cyberbezpieczeństwie



Definicja i zakres sektora

Sektor cyberbezpieczeństwa obejmuje podmioty/organizacje/osoby prowadzące działania w celu ochrony systemów informacyjnych, usług i produktów przed cyberzagrożeniami dla zapewnienia niezakłóconego funkcjonowania podmiotów/organizacji/osób.

Przy czym przez:
Cyberzagrożenia rozumie się wszelkie potencjalne okoliczności, zdarzenia lub działania, które mogą wyrządzić szkodę w systemach informacyjnych, spowodować zakłócenia w nich lub w inny sposób niekorzystnie wpłynąć na te oraz ich interesariuszy.

Działania w celu ochrony systemów rozumie się czynności wykonywane na etapach identyfikacji, ochrony, wykrywania, reakcji, odbudowy procesu cyberbezpieczeństwa oraz audytu; działania te realizowane są zarówno podczas wdrażania systemu, jego eksploatacji, jak i wycofania tego systemu z użytkowania.

System informacyjny rozumie się jako wielopoziomową strukturę, obejmującą komponenty techniczne i organizacyjne, pozwalającą na przetwarzanie informacji wejściowych w wyjściowe.

Wyznaczniki sektora – główne obszary działalności sektora

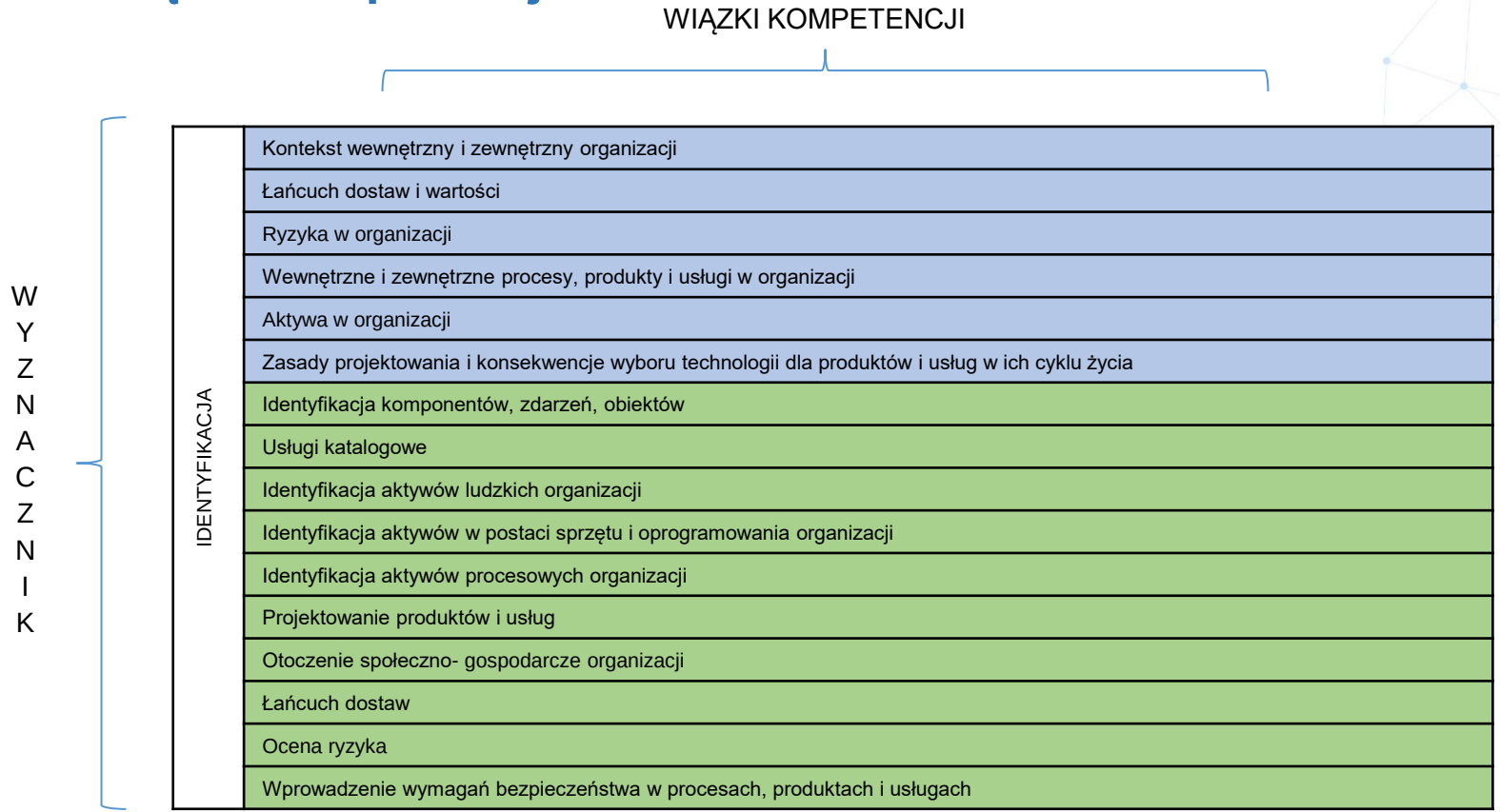
przekrojowe obszary, których nie można jednoznacznie przypisać do ww. wyznaczników

Wstępne wymagania dla cyberbezpieczeństwa
Identyfikacja
Ochrona
Wykrywanie
Reakcja
Odbudowa
Audyt cyberbezpieczeństwa w ramach zarządzania bezpieczeństwem
Standardy pracy
Komunikacja i współpraca

za ENISA, NIST, odnoszą się do procesu zapewniania bezpieczeństwa

kompetencje społeczne

Wiązki kompetencji



Charakterystyki poziomów

NAZWA WIĄZKI	POZIOM 3	POZIOM 4	POZIOM 5	POZIOM 6	POZIOM 7	POZIOM 8
Szkodliwe oprogramowania	podstawowe typy szkodliwego oprogramowania	zasady statycznej i dynamicznej analizy szkodliwego oprogramowania, w tym analizy w systemach sandbox, kodu maszynowego	sposób działania szkodliwego oprogramowania używanego przez atakujacych			

NAZWA WIĄZKI	POZIOM 3	POZIOM 4	POZIOM 5	POZIOM 6	POZIOM 7	POZIOM 8
Analiza szkodliwego oprogramowania i systemów informatycznych	identyfikować typy szkodliwego oprogamowania wyszukiwać informacje o szkodliwym oprogramowaniu i wykorzystywanych przez niego narzędziach	identyfikować słabe punkty w systemach informatycznych wykorzystywane przez szkodliwe oprogramowanie	analizować szkodliwe oprogramowanie oraz słabe punkty w systemach informatycznych	analizować trendy dotyczące szkodliwego oprogramowania	modyfikować szkodliwe oprogramowanie w celu zwiększenia ochrony systemów	opracować metody zabezpieczania systemów informatycznych przed nieznanym szkodliwym oprogramowaniem

NAZWA WIĄZKI	POZIOM 3	POZIOM 4	POZIOM 5	POZIOM 6	POZIOM 7	POZIOM 8
Odpowiedzialność		świadomego przestrzegania zasad i procedur cyberbezpieczeństwa, z uwzględnieniem ewentualnych konskwencji nierzetelnego wykonywania zadań	ponoszenia konsekwencji za nierzetelne wykonywanie zadań lub nieprzestrzegania zasad i procedur cyberbezpieczeństwa	promowania postawy odpowiedzialności za procesy zapewniania cyberbezpieczestwa	współtworzenia norm/standardów zachowań projakościowych w obszarze cyberbezpieczeństwa promowania kultury projakościowej w obszarze cyberbezpieczeństwa	kształtowania kultury projakościowej w obszarze cyberbezpieczeństwa

WYZNACZNI		NAZWA WIĄZKI	POZIOM 3	POZIOM 4	POZIOM 5	POZIOM 6	POZIOM 7	POZIOM 8
Odbudowa	WIEDZA: znai rozumie	Kopie bezpieczeństwa	rodzaje kopii bezpieczeństwa	budowę i ograniczenia nośników danych metody i systemy wykonywania kopii bezpieczeństwa	zasady budowania zapasowych centrów przetwarzania danych			
		Model ciągłości działania		budowę i ograniczenia modelu ciągłości działania metody wdrażania modelu ciągłości działania	metody opracowywania modelu ciągłości działania dopasowanego do potrzeb organizacji potencjalne skutki incydentu dla działania modelu ciągłości działania			
	UMIEJĘTNOŚCI: potrafi	Identyfikacja zagadnień ciągłości działania	identyfikować rodzaj incydentu	oceniać skalę zagrożenia	reagować na incydent zgodnie z wewnętrznymi procedurami wprowadzać zmiany w przypadku awarii w celu odtworzenia systemu monitorować poprawność działania systemów zapasowych	opracowywać i wdrażać procedury przełączenia na systemy zapasowe		
		Ocena incydentu	replikować incydent	replikować incydent w ramach weryfikacji działania procedur	analizować incydent i jego skutki	opracować rozwiązania strukturalne w odpowiedzi na zaistniały incydent	rekomendować i inicjować wdrożenie zmian strukturalnych	
		Odbudowa modelu ciągłości działania	identyfikować podatności modelu działania w kontekście zaistniałego incydentu	opracować propozycje zmian technicznych w odpowiedzi na zaistniały incydent	analizować sytuację pod kątem zaistniałego incydentu oraz wyciągać wnioski opracować optymalną kolejność działań naprawczych z uwzględnieniem specyfiki organizacji lub systemów wprowadzać korekty do modelu działania	modyfikować modele działania z uwzględnieniem uwarunkowań organizacji i zaistniałego incydentu	tworzyć nowe modele działania z uwzględnieniem uwarunkowań organizacji i zaistniałego incydentu	
		Odtworzenie ciągłości działania	monitorować wskaźniki systemów kontroli działania oraz automatyczne wykonywanie kopii bezpieczeństwa sprawdzać poprawność kopii bezpieczeństwa odtworzyć kopie bezpieczeństwa	monitorować przełączenie się systemów informatycznych na serwery w zapasowym CPD monitorować moment odzyskania pełnej sprawności świadczonych usług przez systemy cyfrowe	rekomendować urządzenia oraz oprogramowanie do wykonywania kopii bezpieczeństwa opracować zasady retencji kopii bezpieczeństwa opracować plan ciągłości działania	dokonywać krytycznej analizy stosowanych rozwiązań w zakresie polityki tworzenia kopii bezpieczeństwa wdrażać zmiany w rozwiązaniach z zakresu tworzenia kopii bezpieczeństwa wynikających z przeprowadzonej ewaluacji polityki dokonywać adaptacji ciągłości działania w ujęciu taktycznym	wdrażać zmiany w rozwiązaniach z zakresu tworzenia kopii bezpieczeństwa wynikających z przeprowadzonej analizy trendów dokonywać adaptacji planu ciągłości działania w ujęciu strategicznym	
		Weryfikacja zapisów umów	identyfikować zapisy umów wpływające na zapewnianie ciągłości działania systemów	weryfikować zgodność zapisów umów z działaniami zapewnieniającymi bezpieczeństwo systemów realizować umowy, w tym OLA i SLA monitorować realizację zapisów umów, w tym OLA i SLA	rekomendować zapisy w umowach, w tym OLA i SLA, wspierające zapewnianie ciągłości działania			

ZINTEGROWANY SYSTEM KWALIFIKACJI

Sektorowa Rama Kwalifikacji dla sektora CYBER w liczbach

9
obszarów kluczowych

108
procesów

ponad **750**
kompetencji

10 ekspertów

ponad **100**
konsultantów

78
zdefiniowanych pojęć

Praktyczne wykorzystanie SRK zdaniem ekspertów CYBER

Identyfikacja luk kompetencyjnych

- podczas procesu rekrutacji można stosować matrycę do oceny umiejętności kandydatów
- śledzenie postępów w nauce i poszukiwanie nowych obszarów rozwoju wśród studentów

Organizacja szkoleń

- skraca czas przygotowania programów edukacyjnych
- wspiera projektowanie programów wzmacniania świadomości na temat zagrożeń wśród uczniów

Zarządzanie zespołem

- sprawne zarządzanie ryzykiem w organizacji
- matryca może pomóc w określeniu wymaganych umiejętności i kompetencji dla zespołu projektowego

ZINTEGROWANY SYSTEM KWALIFIKACJI

IBE INSTYTUT BADAŃ EDUKACYJNYCH

Instytut Badań Edukacyjnych
ul. Górczewska 8, 01-180 Warszawa
tel.: (22) 241 71 00, e-mail: zsk@ibe.edu.pl

Fundusze Europejskie Wiedza Edukacja Rozwój
Rzeczpospolita Polska
IBE kwalifikacje dla każdego
Unia Europejska Europejski Fundusz Społeczny