Warszawa, 26.05.2026r.

Opinia ekspercka do projektu rozporządzenia w sprawie sektorowej ramy kwalifikacji w sektorze cyberbezpieczeństwa

1. WPROWADZENIE

Projekt sektorowej ramy kwalifikacji (SRK) w sektorze cyberbezpieczeństwa należy analizować w kontekście fundamentalnych zmian zachodzących we współczesnym środowisku technologicznym, gospodarczym i bezpieczeństwa. Postępująca cyfryzacja procesów społecznych i ekonomicznych, rosnąca zależność państw oraz organizacji od systemów informatycznych, a także dynamiczny rozwój technologii takich jak chmura obliczeniowa, sztuczna inteligencja czy Internet Rzeczy powodują, że cyberbezpieczeństwo staje się jednym z kluczowych filarów funkcjonowania współczesnych społeczeństw.

Wraz z rosnącym znaczeniem cyberprzestrzeni obserwuje się jednocześnie eskalację zagrożeń – zarówno pod względem ich liczby, jak i złożoności. Współczesne zagrożenia cybernetyczne nie mają już wyłącznie charakteru technicznego, lecz coraz częściej przyjmują formę wieloetapowych operacji, łączących aspekty technologiczne, organizacyjne oraz społeczne. W konsekwencji cyberbezpieczeństwo przestaje być domeną wyłącznie specjalistów IT, a staje się obszarem wymagającym zintegrowanych kompetencji obejmujących analizę danych, zarządzanie ryzykiem, podejmowanie decyzji oraz projektowanie rozwiązań systemowych.

W tych warunkach szczególnego znaczenia nabiera wyzwanie właściwego definiowania, kształtowania i walidacji kompetencji w obszarze cyberbezpieczeństwa. Tradycyjne modele edukacji i opisu kompetencji, oparte na stabilnych i relatywnie powoli zmieniających się dziedzinach wiedzy, okazują się niewystarczające w kontekście dynamicznie ewoluującego środowiska technologicznego. Pojawia się zatem potrzeba stworzenia narzędzi systemowych, które umożliwią uporządkowanie kompetencji w sposób jednocześnie trwały i elastyczny.

Ramy kwalifikacji – zarówno krajowe, jak i sektorowe – pełnią w tym kontekście kluczową rolę. Stanowią one mechanizm porządkujący efekty uczenia się poprzez ich klasyfikację na różnych poziomach złożoności oraz umożliwiający ich odniesienie do wymagań rynku pracy. W przypadku cyberbezpieczeństwa funkcja ta nabiera szczególnego znaczenia ze względu na konieczność zapewnienia spójności pomiędzy edukacją formalną, szkoleniami specjalistycznymi, certyfikacją zawodową oraz praktyką operacyjną.

Sektorowa rama kwalifikacji w cyberbezpieczeństwie powinna zatem pełnić rolę pomostu pomiędzy tymi obszarami, umożliwiając:

- systematyzację wiedzy i umiejętności w formie spójnych kategorii kompetencyjnych,
- budowę ścieżek rozwoju zawodowego w warunkach dynamicznych zmian technologicznych,
- oraz praktyczne wykorzystanie w organizacjach w procesach rekrutacji, oceny i rozwoju pracowników.

Jednocześnie należy podkreślić, że projektowanie ram kwalifikacji w obszarze cyberbezpieczeństwa wiąże się ze specyficznymi wyzwaniami, które odróżniają tę dziedzinę od wielu innych sektorów. Do najważniejszych z nich należą:

- wysoka dynamika zmian technologicznych i organizacyjnych,
- nieprzewidywalny charakter zagrożeń i ich ciągła ewolucja,
- silne powiązanie kompetencji z praktyką operacyjną,
- oraz wysoki poziom specjalizacji ról zawodowych.

W rezultacie tradycyjne podejście do tworzenia ram kwalifikacji, oparte na statycznym opisie wiedzy i umiejętności, może okazać się niewystarczające. Wymagane jest podejście bardziej elastyczne, uwzględniające zdolność adaptacji do nowych warunków oraz orientację na kompetencje o charakterze funkcjonalnym, a nie jedynie technicznym.

Celem niniejszej opinii jest pogłębiona analiza projektu sektorowej ramy kwalifikacji w sektorze cyberbezpieczeństwa z perspektywy eksperckiej, obejmująca zarówno aspekt metodologiczny, jak i operacyjny. Analiza ta koncentruje się na ocenie:

- zgodności projektu z realiami funkcjonowania środowiska cyberbezpieczeństwa,
- trwałości i odporności przyjętych rozwiązań na zmiany technologiczne,
- oraz możliwości praktycznego wykorzystania SRK przez różne grupy interesariuszy, w tym organizacje, instytucje edukacyjne oraz specjalistów.

Projekt SRK ma charakter rozszerzony i w znacznym stopniu operacyjny, co zwiększa jego użyteczność praktyczną, jednak jednocześnie ogranicza jego uniwersalność oraz trwałość regulacyjną jako elementu systemu kwalifikacji.

W dalszej części opracowania przedstawiona zostanie ocena ogólna projektu, a następnie szczegółowa analiza kluczowych wyzwań i ograniczeń, uzupełniona o rekomendacje dotyczące kierunków jego dalszego rozwoju.

2. OCENA OGÓLNA PROJEKTU W UJĘCIU EKSPERCKIM

Projekt sektorowej ramy kwalifikacji w sektorze cyberbezpieczeństwa należy ocenić jako inicjatywę o istotnym znaczeniu systemowym, wpisującą się w szerszy kontekst budowy gospodarki cyfrowej oraz wzmacniania zdolności państwa i organizacji do przeciwdziałania zagrożeniom w przestrzeni cybernetycznej. W warunkach rosnącej złożoności systemów informacyjnych oraz zwiększającej

się skali i intensywności zagrożeń, uporządkowanie kompetencji w tym obszarze stanowi działanie zarówno uzasadnione, jak i konieczne.

Na poziomie ogólnym projekt SRK należy uznać za poprawny koncepcyjnie. Dokument podejmuje próbę kompleksowego ujęcia cyberbezpieczeństwa jako obszaru obejmującego zróżnicowane komponenty – od infrastruktury technicznej (IT, OT, IoT), poprzez procesy operacyjne i zarządcze, aż po uwarunkowania prawne i organizacyjne. Tak szerokie ujęcie należy ocenić pozytywnie, ponieważ odpowiada rzeczywistemu, wielowymiarowemu charakterowi cyberbezpieczeństwa.

Z punktu widzenia praktyki szczególnie istotne jest odwzorowanie logiki cyklu życia bezpieczeństwa, obejmującego fazy identyfikacji, ochrony, detekcji, reagowania i odtwarzania (identify–protect–detect–respond–recover). Cykl ten stanowi fundament współczesnych modeli zarządzania bezpieczeństwem i jest powszechnie stosowany zarówno w standardach międzynarodowych, jak i w praktyce organizacyjnej. Uwzględnienie tego podejścia w SRK wzmacnia jej zgodność z realiami funkcjonowania systemów bezpieczeństwa.

Jednocześnie należy zauważyć, że zastosowanie modelu cyklicznego ma przede wszystkim charakter konceptualny i nie jest w pełni konsekwentnie odwzorowane na poziomie szczegółowych opisów kompetencji. O ile struktura ogólna dokumentu wskazuje na poprawne rozumienie logiki bezpieczeństwa, o tyle na poziomie operacyjnym pojawiają się niespójności, które utrudniają jednoznaczne przypisanie kompetencji do poszczególnych faz cyklu.

Z perspektywy metodologicznej projekt SRK wykazuje również ambiwalencję pomiędzy dążeniem do szczegółowego odwzorowania praktyki a koniecznością zachowania charakteru ramowego. W wielu fragmentach dokumentu widoczna jest tendencja do schodzenia na poziom operacyjny, obejmujący konkretne techniki, narzędzia oraz procedury. Choć takie podejście może zwiększać czytelność dla użytkowników mniej zaawansowanych, w dłuższej perspektywie prowadzi ono do ograniczenia trwałości dokumentu oraz utrudnia jego adaptację do zmian technologicznych.

W konsekwencji SRK znajduje się w stanie napięcia pomiędzy dwoma funkcjami:

- funkcją **deskryptywną**, polegającą na odwzorowaniu aktualnego stanu praktyki cyberbezpieczeństwa,
- funkcją **ramową**, polegającą na definiowaniu uniwersalnych kategorii kompetencyjnych.

Analiza projektu wskazuje, że obecnie dominujące jest podejście deskryptywne, co stanowi jedno z głównych źródeł jego ograniczeń.

Na poziomie użyteczności systemowej należy zauważyć, że projekt SRK posiada potencjał integracyjny, umożliwiający powiązanie różnych obszarów funkcjonowania rynku pracy i systemu edukacyjnego. Może on stanowić punkt odniesienia dla:

- programów kształcenia formalnego,
- szkoleń specjalistycznych,
- systemów certyfikacji,
- oraz procesów zarządzania kompetencjami w organizacjach.

Jednakże potencjał ten nie jest w pełni wykorzystany ze względu na brak wystarczająco czytelnych mechanizmów powiązania pomiędzy kompetencjami a rzeczywistymi rolami zawodowymi oraz strukturami organizacyjnymi. W obecnej formie dokument stanowi raczej zbiór opisów kompetencji niż narzędzie umożliwiające ich bezpośrednie zastosowanie w praktyce zarządczej.

Istotnym elementem oceny ogólnej jest również analiza trwałości regulacyjnej dokumentu. Cyberbezpieczeństwo jako dziedzina charakteryzuje się wyjątkowo szybkim tempem zmian, co powoduje, że wiele rozwiązań technologicznych i operacyjnych ulega dezaktualizacji w stosunkowo krótkim czasie. W przypadku SRK oznacza to konieczność projektowania jej w sposób odporny na zmiany, co wymaga unikania nadmiernego uzależnienia od bieżących technologii.

W obecnym kształcie dokument w ograniczonym stopniu spełnia ten warunek, co wynika z wysokiego poziomu operacyjności niektórych opisów kompetencji. Wprowadzenie licznych odniesień do konkretnych rozwiązań technologicznych ogranicza jego uniwersalność i zwiększa ryzyko dezaktualizacji. W dłuższej perspektywie może to prowadzić do konieczności częstych nowelizacji lub do stopniowej utraty znaczenia SRK jako punktu odniesienia dla systemu kompetencji.

Podsumowując, projekt sektorowej ramy kwalifikacji w sektorze cyberbezpieczeństwa należy ocenić jako:

- **trafny koncepcyjnie**,
- **poprawny w zakresie ogólnej struktury**,
- **spójny z uznanymi modelami zarządzania bezpieczeństwem**,

jednocześnie jednak:

- obciążony nadmiernym poziomem szczegółowości,
- niewystarczająco zorientowany na trwałe kompetencje,
- oraz wymagający doprecyzowania w zakresie użyteczności operacyjnej.

Ocena ta stanowi punkt wyjścia do dalszej, pogłębionej analizy wyzwań przedstawionych w kolejnych podrozdziałach, w których szczegółowo omówione zostały kluczowe ograniczenia SRK oraz ich implikacje dla praktyki cyberbezpieczeństwa.

3. KLUCZOWE WYZWANIA Z PERSPEKTYWY EKSPERTA DS. CYBERBEZPIECZEŃSTWA

3.1. Nadmierna operacjonalizacja kompetencji – ryzyko „technicyzacji" SRK

Jednym z podstawowych wyzwań analizowanego projektu sektorowej ramy kwalifikacji jest wysoki poziom operacyjnej szczegółowości opisów efektów uczenia się. W wielu miejscach dokument odnosi się bezpośrednio do konkretnych technik, narzędzi oraz procedur stosowanych w praktyce cyberbezpieczeństwa. Takie podejście, choć potencjalnie użyteczne w kontekście projektowania programów szkoleniowych lub specyfikacji kursów, w przypadku ram kwalifikacji prowadzi do istotnych konsekwencji metodologicznych.

Z perspektywy teorii ram kwalifikacji kluczowe znaczenie ma rozróżnienie pomiędzy kompetencją jako zdolnością o charakterze trwałym, a jej implementacją techniczną, która ma charakter zmienny i kontekstowy. Wprowadzanie do SRK odniesień do konkretnych rozwiązań technologicznych prowadzi do zjawiska, które można określić jako „technicyzację regulacji". Oznacza ono sytuację, w której dokument zaczyna odwzorowywać bieżący stan praktyki technicznej, zamiast definiować uniwersalne zdolności pozwalające na funkcjonowanie w zmieniającym się środowisku.

Konsekwencje takiego podejścia są wielowymiarowe. Po pierwsze, dochodzi do skrócenia cyklu życia dokumentu, ponieważ technologie wykorzystywane w cyberbezpieczeństwie podlegają szybkim zmianom. Po drugie, ograniczona zostaje możliwość adaptacji SRK do nowych obszarów technologicznych, takich jak sztuczna inteligencja, systemy rozproszone czy rozwiązania post-kwantowe. Po trzecie, dochodzi do przesunięcia funkcji dokumentu – zamiast pełnić rolę ramy kwalifikacji, zaczyna on przypominać katalog kompetencji technicznych lub standard szkoleniowy.

W praktyce operacyjnej cyberbezpieczeństwa kompetencje specjalistów mają charakter znacznie bardziej uniwersalny. Analityk SOC nie jest definiowany przez znajomość konkretnego narzędzia, lecz przez zdolność interpretacji zdarzeń. Specjalista reagowania na incydenty nie opiera się wyłącznie na znajomości procedur, lecz na umiejętności rekonstrukcji zdarzeń i podejmowania decyzji. Podobnie w red teamingu kluczowa jest zdolność modelowania przeciwnika, a nie jedynie znajomość technik.

W konsekwencji obecny poziom operacjonalizacji SRK należy uznać za nieadekwatny do jej funkcji systemowej. Konieczne jest przesunięcie poziomu opisu z warstwy narzędzi i technik na warstwę kompetencji, które mają charakter bardziej trwały i uniwersalny. Z perspektywy systemu kwalifikacji oznacza to ograniczenie przenaszalności efektów uczenia się oraz osłabienie neutralności technologiczno-metodologicznej dokumentu.

3.2. Niedostosowanie do dynamiki zagrożeń cybernetycznych

Jednym z fundamentalnych wyzwań w projektowaniu sektorowej ramy kwalifikacji (SRK) w obszarze cyberbezpieczeństwa jest uwzględnienie specyfiki samej domeny, która charakteryzuje się wyjątkowo wysoką dynamiką zmian. W przeciwieństwie do wielu innych obszarów regulacyjnych, cyberbezpieczeństwo rozwija się w sposób nieliniowy, gdzie zmiany technologiczne, nowe modele architektoniczne oraz ewoluujące strategie ataków prowadzą do ciągłego redefiniowania wymagań kompetencyjnych.

Analizowany projekt SRK, choć obejmuje szeroki zakres zagadnień, w dużej mierze koncentruje się na opisie znanych kategorii zagrożeń oraz istniejących technik i podejść. Takie podejście – typowe dla dokumentów o charakterze deskryptywnym – nie oddaje jednak istoty pracy specjalisty cyberbezpieczeństwa, który w praktyce operuje w warunkach niepewności i zmienności.

Z punktu widzenia eksperta kluczowe znaczenie mają kompetencje umożliwiające funkcjonowanie w środowisku nieprzewidywalnym, w szczególności:

- zdolność identyfikacji anomalii i nietypowych wzorców zachowań,

- umiejętność formułowania hipotez analitycznych,
- oraz zdolność szybkiego dostosowania się do nowych typów zagrożeń.

W praktyce operacyjnej zjawisko to jest szczególnie widoczne w środowiskach takich jak:

- SOC (Security Operations Center), gdzie analitycy coraz rzadziej operują w oparciu o znane sygnatury zagrożeń, a coraz częściej analizują subtelne anomalie w ruchu sieciowym lub zachowaniu użytkowników;
- blue team, gdzie identyfikacja zagrożeń opiera się na interpretacji wskaźników zachowania (IoB), a nie wyłącznie na znanych wskaźnikach kompromitacji (IoC);
- red team, gdzie specjaliści tworzą nowe scenariusze ataków poprzez kreatywne łączenie istniejących technik, często wykraczając poza znane modele zagrożeń;
- zespoły CSIRT, w których każdy incydent ma charakter unikalny i wymaga rekonstruowania przebiegu zdarzeń na podstawie niepełnych danych.

W konsekwencji SRK częściowo koncentruje się na opisie znanych kategorii zagrożeń, co może ograniczać jej zdolność do wspierania rozwoju kompetencji o charakterze adaptacyjnym i przyszłościowym.

3.3. Ograniczona użyteczność operacyjna SRK

Niedostosowanie SRK do dynamiki zagrożeń znajduje swoje bezpośrednie odzwierciedlenie w jej ograniczonej użyteczności operacyjnej. Choć dokument prezentuje szeroki wachlarz kompetencji, nie zapewnia wystarczająco przejrzystego powiązania pomiędzy tymi kompetencjami a rzeczywistymi rolami i zadaniami wykonywanymi w organizacjach.

Cyberbezpieczeństwo w praktyce ma charakter silnie zróżnicowany i opiera się na wyspecjalizowanych rolach, takich jak:

- analityk SOC,
- specjalista reagowania na incydenty (Incident Responder),
- pentester / red teamer,
- architekt bezpieczeństwa,
- specjalista GRC.

Brak bezpośredniego odwzorowania tych ról w strukturze SRK prowadzi do szeregu konsekwencji.

W środowisku SOC różne poziomy analityków realizują odmienne zadania – od triage alertów po zaawansowane threat hunting. SRK nie umożliwia jednak jednoznacznego przypisania kompetencji do tych poziomów.

W zespołach CSIRT kluczowe są kompetencje decyzyjne i analityczne, związane z działaniem w sytuacjach kryzysowych. Dokument nie eksponuje wystarczająco tych zdolności.

W przypadku blue teamingu istotne jest przetwarzanie dużych wolumenów danych i identyfikacja subtelnych zależności, co wymaga wysokiego poziomu kompetencji interpretacyjnych.

W red teamingu dominują kompetencje kreatywne i symulacyjne, związane z modelowaniem przeciwnika – aspekt ten nie znajduje wystarczającego odzwierciedlenia w SRK.

W rezultacie dokument:

- może trudny do wykorzystania w procesach rekrutacji i oceny kompetencji,
- nie wspiera efektywnie planowania ścieżek kariery,
- oraz ma ograniczoną użyteczność w zarządzaniu zespołami bezpieczeństwa.

Jednocześnie należy wskazać, że obecny poziom szczegółowości może zwiększać jego użyteczność w kontekście analiz kompetencyjnych oraz projektowania programów szkoleniowych.

3.4. Niedostateczne rozróżnienie warstw kompetencyjnych

Istotnym ograniczeniem analizowanego projektu sektorowej ramy kwalifikacji jest niewystarczająco precyzyjne i konsekwentne rozróżnienie warstw kompetencyjnych, które w praktyce cyberbezpieczeństwa mają charakter fundamentalny.

Z punktu widzenia zarządzania bezpieczeństwem oraz organizacji pracy w zespołach cyberbezpieczeństwa kompetencje można jednoznacznie przypisać do trzech poziomów:

- operacyjnego, obejmującego działania techniczne i wykonawcze,
- analitycznego, obejmującego interpretację danych i identyfikację wzorców,
- strategicznego, obejmującego projektowanie systemów bezpieczeństwa i zarządzanie ryzykiem.

Projekt SRK nie odwzorowuje tej struktury w sposób spójny. W opisach kompetencji często mieszane są elementy wymagające różnych poziomów wiedzy i odpowiedzialności, co prowadzi do niejednoznaczności interpretacyjnych.

W praktyce operacyjnej wyzwanie to jest szczególnie widoczne w środowiskach takich jak SOC, gdzie funkcjonują jasno określone poziomy zaawansowania (L1–L3), oraz w zespołach CSIRT, gdzie rozróżnienie pomiędzy działaniem technicznym a podejmowaniem decyzji strategicznych ma kluczowe znaczenie.

Brak jednoznacznego rozróżnienia warstw kompetencyjnych skutkuje:

- utrudnieniem projektowania ścieżek kariery,
- ograniczeniem możliwości budowy struktur zespołów,
- oraz obniżeniem przejrzystości systemu kwalifikacji.

Wyzwanie to ma charakter systemowy, ponieważ utrudnia jednoznaczne przypisanie poziomów SRK do progresji kompetencji określonej w PRK.

3.5. Brak dostosowania do modelu lifelong learning i microcredentials

Kolejnym istotnym ograniczeniem projektu jest jego niedostosowanie do współczesnego modelu rozwoju kompetencji, opartego na idei uczenia się przez całe życie oraz rosnącej roli mikrokwalifikacji.

Cyberbezpieczeństwo jest obszarem, w którym dezaktualizacja wiedzy następuje wyjątkowo szybko, co wymusza ciągłe doskonalenie kompetencji. W praktyce oznacza to przejście od modelu liniowego kształcenia do modelu iteracyjnego, opartego na krótkich i wyspecjalizowanych formach edukacyjnych.

Model ten obejmuje:

- certyfikacje branżowe,
- kursy specjalistyczne,
- mikrokwalifikacje potwierdzające konkretne umiejętności.

Struktura SRK, mająca charakter relatywnie monolityczny i oparta na progresji poziomów, w ograniczonym stopniu odzwierciedla tę dynamikę.

W konsekwencji:

- ograniczona jest możliwość wykorzystania SRK w systemach szkoleniowych,
- utrudniona jest integracja z certyfikacją branżową,
- oraz zmniejszona jest jej użyteczność w realiach rynku pracy.

Z perspektywy eksperckiej konieczne jest dostosowanie SRK do modelu lifelong learning poprzez zwiększenie jej modularności oraz umożliwienie definiowania kompetencji cząstkowych.

4. REKOMENDACJE EKSPERCKIE

4.1. Reorientacja SRK na poziom kompetencyjny (a nie narzędziowy)

Podstawowym kierunkiem zmian, wynikającym bezpośrednio z wcześniej zidentyfikowanych ograniczeń SRK, jest konieczność przejścia od podejścia narzędziowego do podejścia kompetencyjnego. w obecnym kształcie dokument wykazuje wyraźną tendencję do definiowania efektów uczenia się poprzez odniesienia do konkretnych narzędzi, technologii oraz technik operacyjnych, co wskazuje na przesunięcie opisu z poziomu kompetencji ogólnych na poziom działań operacyjnych, co prowadzi do nadmiernego zakotwiczenia SRK w bieżącym stanie praktyki technologicznej.

Z metodologicznego punktu widzenia takie podejście jest nieadekwatne do charakteru ram kwalifikacji. Kompetencje powinny być definiowane jako zdolności o charakterze trwałym,

obejmujące integrację wiedzy, umiejętności oraz postaw, a nie jako znajomość konkretnych implementacji technologicznych. Narzędzia, metody i techniki ulegają bowiem szybkim zmianom, natomiast kompetencje funkcjonalne zachowują swoją aktualność nawet w obliczu transformacji technologicznych.

W tym kontekście szczególnego znaczenia nabiera redefinicja efektów uczenia się w kierunku zdolności takich jak:

identyfikacja i analiza podatności w złożonych systemach informatycznych,
interpretacja zdarzeń bezpieczeństwa w warunkach niepewności i niekompletnych danych,
ocena ryzyka oraz jego wpływu na funkcjonowanie organizacji,
dobór adekwatnych metod detekcji i reagowania,
projektowanie i implementacja mechanizmów zabezpieczających.

Znaczenie takiego podejścia jest szczególnie widoczne w środowiskach operacyjnych. W **SOC (Security Operations Center)** analitycy nie operują wyłącznie na poziomie obsługi narzędzi SIEM czy XDR, lecz przede wszystkim na poziomie interpretacji danych i identyfikacji wzorców anomalii. W zespołach **CSIRT** kluczowa jest zdolność rekonstrukcji przebiegu incydentu oraz podejmowania decyzji w warunkach braku pełnej informacji. W przypadku **red teamingu** zasadnicze znaczenie ma zdolność modelowania przeciwnika i kreatywnego konstruowania scenariuszy ataków, a nie jedynie znajomość katalogu technik.

Przejście na poziom kompetencyjny prowadzi do:

- zwiększenia trwałości SRK w czasie,
- uniezależnienia jej od zmiennych technologii,
- oraz umożliwienia jej zastosowania w różnych środowiskach organizacyjnych.

W szczególności rekomenduje się zastąpienie odniesień do konkretnych technik i narzędzi ich kategoriami funkcjonalnymi, takimi jak: mechanizmy uwierzytelniania, kontrola dostępu, walidacja danych oraz analiza zdarzeń bezpieczeństwa.

Podejście takie zwiększa trwałość SRK oraz jej neutralność technologiczno-metodologiczną, a także poprawia przenaszalność efektów uczenia się pomiędzy różnymi środowiskami technologicznymi.

4.2. Wprowadzenie adaptacyjnego modelu aktualizacji SRK

Drugim kluczowym elementem transformacji SRK powinno być wprowadzenie adaptacyjnego modelu jej aktualizacji, który odpowiadałby specyfice cyberbezpieczeństwa jako dziedziny podlegającej dynamicznym i często nieprzewidywalnym zmianom.

Obecna konstrukcja SRK ma charakter statyczny i reprezentuje stan wiedzy na określony moment, co w przypadku cyberbezpieczeństwa stanowi poważne ograniczenie. W praktyce operacyjnej nowe techniki ataków, zmiany w architekturze systemów oraz rozwój narzędzi bezpieczeństwa pojawiają się w tempie znacznie szybszym niż cykle legislacyjne.

Adaptacyjny model aktualizacji powinien mieć charakter formalny i obejmować trzy zasadnicze komponenty:

- **cykliczne przeglądy SRK**, realizowane w określonych interwałach czasowych (np. co 2–3 lata),
- **systematyczne konsultacje ze środowiskiem eksperckim**, obejmujące praktyków cyberbezpieczeństwa (SOC, CSIRT, red/blue team),
- **ciągły monitoring trendów technologicznych i zagrożeń**, pozwalający identyfikować nowe obszary kompetencyjne.

W praktyce oznacza to zdolność SRK do reagowania na zmiany takie jak:

- rozwój zagrożeń opartych na sztucznej inteligencji (AI-driven attacks),
- transformacja architektury systemów w kierunku rozwiązań chmurowych i rozproszonych,
- ewolucja narzędzi (np. przejście od SIEM do XDR i platform analitycznych opartych na AI).

Przykładowo:

- w środowisku **SOC** rozwój detekcji behawioralnej wymaga redefinicji kompetencji analitycznych,
- w **red teamingu** pojawiają się nowe modele symulacji przeciwnika,
- w **blue teamingu** rośnie znaczenie identyfikacji wzorców zachowań zamiast klasycznych wskaźników kompromitacji.

Brak adaptacyjności prowadzi do sytuacji, w której SRK traci aktualność i zaczyna odzwierciedlać przeszłość, zamiast wspierać rozwój kompetencji przyszłościowych. Mechanizm ten powinien być osadzony w procedurach przeglądu regulacji sektorowych, co zapewni jego trwałość instytucjonalną oraz skuteczność wdrożeniową.

4.3. Budowa architektury modułowej

Najbardziej kompleksową odpowiedzią na zidentyfikowane wyzwania strukturalne SRK jest wprowadzenie architektury modułowej, odzwierciedlającej rzeczywisty charakter cyberbezpieczeństwa jako zbioru wyspecjalizowanych obszarów kompetencyjnych.

Cyberbezpieczeństwo w praktyce nie funkcjonuje jako jednolita ścieżka kompetencyjna, lecz jako ekosystem specjalizacji, które rozwijają się częściowo niezależnie. W związku z tym model liniowy, oparty wyłącznie na progresji poziomów, nie oddaje rzeczywistej struktury tej dziedziny.

Podejście modułowe zakłada podział SRK na autonomiczne, lecz powiązane obszary funkcjonalne, takie jak:

- **operacje bezpieczeństwa (SOC / Blue Team)** – monitoring, analiza zdarzeń, detekcja zagrożeń,

- **testowanie bezpieczeństwa i red teaming** – identyfikacja podatności, symulacja ataków,
- **reagowanie na incydenty (CSIRT)** – analiza incydentów, działania kryzysowe,
- **architektura i inżynieria bezpieczeństwa (DevSecOps)** – projektowanie systemów bezpiecznych,
- **zarządzanie bezpieczeństwem (GRC)** – zarządzanie ryzykiem, zgodność, governance.

Każdy z tych modułów:

- odpowiada odrębnemu obszarowi praktyki,
- wymaga wyspecjalizowanych kompetencji,
- może być rozwijany i certyfikowany niezależnie.

W rzeczywistości organizacyjnej dominują właśnie takie wyspecjalizowane role. Rzadko występują stanowiska obejmujące wszystkie obszary jednocześnie, co oznacza, że model modułowy lepiej odzwierciedla strukturę rynku pracy.

Wprowadzenie architektury modułowej umożliwia:

- budowę elastycznych i nieliniowych ścieżek kariery,
- rozwój systemu mikrokwalifikacji,
- łatwiejszą integrację SRK z systemami szkoleniowymi i certyfikacyjnymi,
- oraz zwiększenie jej użyteczności w praktyce organizacyjnej.

Podejście modułowe zwiększa elastyczność SRK oraz umożliwia jej lepsze dostosowanie do zróżnicowanej struktury rynku pracy i specjalizacji w sektorze cyberbezpieczeństwa.

4.4. Integracja z rolami operacyjnymi

Istotnym uzupełnieniem powyższych zmian jest wzmocnienie powiązania SRK z rzeczywistymi rolami zawodowymi funkcjonującymi w cyberbezpieczeństwie. Aktualna postać dokumentu nie zapewnia takiego powiązania, co ogranicza jego użyteczność wdrożeniową.

SRK powinna umożliwiać jednoznaczne odwzorowanie kompetencji na role takie jak:

- analityk SOC (różne poziomy zaawansowania),
- specjalista reagowania na incydenty,
- pentester / red teamer,
- architekt bezpieczeństwa,
- specjalista GRC.

Takie odwzorowanie:

- ułatwia wykorzystanie SRK w procesach HR,
- wspiera planowanie ścieżek kariery,
- oraz zwiększa jej znaczenie praktyczne.

Jednocześnie powiązanie to powinno mieć charakter pomocniczy i interpretacyjny, tak aby nie ograniczać uniwersalności ramy kwalifikacji.

4.5. Wzmocnienie warstwy interpretacyjnej

Ostatnim elementem rekomendowanych zmian jest rozwinięcie warstwy interpretacyjnej SRK. Dokument w obecnej formie ma charakter w dużej mierze deskryptywny, co utrudnia jego praktyczne zastosowanie przez różne grupy użytkowników.

Z punktu widzenia wdrożeniowego zasadne jest uzupełnienie SRK o:

- przewodniki interpretacyjne,
- przykłady zastosowania kompetencji w praktyce,
- słownik pojęć i terminologii.

Takie elementy zwiększają czytelność dokumentu i umożliwiają jego efektywne wykorzystanie zarówno w edukacji, jak i w środowisku organizacyjnym. Rozbudowa warstwy interpretacyjnej powinna mieć charakter nienormatywny, co pozwoli na jej elastyczną aktualizację niezależnie od zmian w samej SRK.

5. UWAGI SZCZEGÓŁOWE ORAZ PROPONOWANE KIERUNKI KOREKTY PROJEKTU SRK

5.1. Zakres wymagający udoskonalenia

5.1.1. Poziom szczegółowości opisu kompetencji

W aktualnej wersji projektu część opisów kompetencji ma charakter operacyjny i odwołuje się do konkretnych praktyk technicznych stosowanych w cyberbezpieczeństwie.

Powoduje to:

- ograniczenie uniwersalności kwalifikacji,
- osłabienie neutralności technologiczno-metodologicznej,
- zmniejszenie trwałości regulacyjnej SRK.

Rekomenduje się:

- zwiększenie poziomu uogólnienia opisów kompetencji,
- przesunięcie akcentu z narzędzi i technik na zdolności funkcjonalne,
- pozostawienie przykładów operacyjnych w materiałach pomocniczych.

5.1.2. Struktura poziomów kwalifikacji

Projekt SRK nie zawsze zapewnia jednoznaczne rozróżnienie progresji kompetencyjnej pomiędzy poziomami. Może to prowadzić do:

- niejednoznaczności interpretacyjnej,
- trudności w budowie ścieżek kariery.

Rekomenduje się:

- doprecyzowanie różnic jakościowych między poziomami,
- wyraźniejsze rozróżnienie kompetencji:
    - operacyjnych,
    - analitycznych,
    - strategicznych.

5.1.3. Powiązanie z rolami zawodowymi

Struktura SRK implikuje istnienie ról zawodowych, jednak nie zapewnia ich jednoznacznego odwzorowania. Ogranicza to:

- użyteczność w procesach HR,
- możliwość implementacji w organizacjach.

Rekomenduje się:

- wprowadzenie powiązań kompetencji z rolami zawodowymi,
- umieszczenie ich w warstwie interpretacyjnej, a nie normatywnej.

5.1.4. Mechanizm aktualizacji SRK

Projekt nie przewiduje formalnego mechanizmu aktualizacji.W kontekście dynamicznego rozwoju cyberbezpieczeństwa stanowi to istotne ograniczenie.

Rekomenduje się:

- wprowadzenie cyklicznego przeglądu SRK (np. co 2–3 lata),
- uwzględnienie udziału środowiska eksperckiego,
- powiązanie procesu aktualizacji z monitorowaniem trendów technologicznych.

5.2. Elementy wymagające usunięcia lub ograniczenia

5.2.1. Odniesienia do konkretnych technik i narzędzi

Obecność odniesień do konkretnych rozwiązań technicznych powoduje uzależnienie SRK od bieżącego stanu technologii. **Rekomenduje się:**

- ograniczenie takich odniesień,
- zastąpienie ich kategoriami funkcjonalnymi kompetencji.

5.2.2. Nadmiernie operacyjny sposób opisu

Część zapisów przyjmuje charakter:

- instrukcyjny,
- zadaniowy.

Może to prowadzić do przesunięcia funkcji SRK w stronę standardu zawodowego.

Rekomenduje się:

- ograniczenie opisów czynności operacyjnych,
- stosowanie języka kompetencyjnego (analizuje, ocenia, projektuje).

5.2.3. Zamknięte katalogi kompetencji

Niektóre fragmenty mają charakter katalogów zamkniętych.

Ogranicza to:

- elastyczność,
- zdolność adaptacyjną SRK.

Rekomenduje się:

- stosowanie opisów otwartych i funkcjonalnych,
- unikanie enumeratywnego wyliczania technologii i rozwiązań.

5.3. Elementy wymagające uzupełnienia

5.3.1. Warstwa interpretacyjna

Projekt SRK ma charakter głównie deskryptywny i nie zawiera wystarczających narzędzi wspierających jego stosowanie.

Rekomenduje się uzupełnienie o:

- przewodnik interpretacyjny,
- przykłady zastosowań kompetencji,
- słownik pojęć i terminologii.

5.3.2. Mapowanie kompetencji na role zawodowe

Brakuje czytelnego powiązania SRK z rzeczywistą strukturą rynku pracy.

Rekomenduje się:

- opracowanie map kompetencji do ról zawodowych (np. SOC, CSIRT, GRC),
- udostępnienie ich jako materiałów pomocniczych.

5.3.3. Uwzględnienie modelu lifelong learning

SRK ma charakter głównie liniowy i nie odzwierciedla w pełni współczesnych modeli rozwoju kompetencji.

Rekomenduje się:

- wprowadzenie podejścia modularnego,
- umożliwienie definiowania kompetencji cząstkowych,
- powiązanie SRK z systemami certyfikacji branżowej.

5.3.4. Wzmocnienie odniesienia do PRK

Relacja SRK do Polskiej Ramy Kwalifikacji wymaga doprecyzowania na poziomie interpretacyjnym.

Rekomenduje się:

- jednoznaczne wskazanie progresji kompetencji względem PRK,
- wzmocnienie interoperacyjności systemowej.

5.4. Wniosek syntetyczny

Projekt SRK nie wymaga zmiany kierunku, lecz: **ukierunkowanej korekty metodologicznej i strukturalnej**, polegającej na:

- ograniczeniu poziomu operacyjności,
- zwiększeniu uniwersalności opisów kompetencji,
- wzmocnieniu warstwy interpretacyjnej i adaptacyjnej.

6. WNIOSKI KOŃCOWE

Przeprowadzona analiza projektu sektorowej ramy kwalifikacji w sektorze cyberbezpieczeństwa prowadzi do wniosku, że dokument ten stanowi istotny i potrzebny element budowy systemowego podejścia do rozwoju kompetencji w obszarze bezpieczeństwa cyfrowego. Jego znaczenie wynika zarówno z rosnącej roli cyberbezpieczeństwa w funkcjonowaniu państwa i gospodarki, jak i z konieczności uporządkowania dynamicznie rozwijającego się rynku pracy w tym sektorze.

Na poziomie ogólnym projekt SRK należy uznać za inicjatywę trafną koncepcyjnie i osadzoną w aktualnych realiach transformacji cyfrowej. Dokument podejmuje próbę integracji różnych wymiarów cyberbezpieczeństwa – technicznego, organizacyjnego i prawnego – co odpowiada jego rzeczywistej, wieloaspektowej naturze. Ponadto odwołanie do cyklu życia bezpieczeństwa oraz

próba uporządkowania efektów uczenia się w odniesieniu do poziomów kwalifikacji stanowią ważny krok w kierunku budowy spójnego systemu kompetencyjnego.

Jednocześnie analiza szczegółowa wykazała, że kluczowe ograniczenia projektu wynikają przede wszystkim z przyjętej struktury oraz poziomu abstrakcji opisów kompetencji, przy zachowaniu wysokiej wartości merytorycznej dokumentu. W szczególności zidentyfikowane wyzwania dotyczą:

- wysokiego poziomu operacyjności i technicyzacji zapisów,
- częściowego niedostosowania do dynamicznego i nieprzewidywalnego środowiska zagrożeń,
- konieczności dalszego doprecyzowania użyteczności operacyjnej wynikającej z braku powiązania z realnymi rolami zawodowymi,
- braku wyraźnego rozróżnienia warstw kompetencyjnych,
- oraz niedostosowania do współczesnych modeli rozwoju kompetencji, opartych na lifelong learning i mikrokwalifikacjach.

Wyzwania te mają charakter systemowy i wzajemnie się wzmacniają. Nadmierna szczegółowość prowadzi do spadku trwałości dokumentu, co w warunkach dynamicznych zmian technologicznych powoduje szybkie starzenie się jego zapisów. Brak modularności oraz niedostateczne odwzorowanie ról zawodowych ograniczają jego użyteczność w organizacjach, natomiast niewystarczające rozróżnienie poziomów kompetencyjnych utrudnia budowę spójnych ścieżek kariery.

Z perspektywy funkcjonalnej oznacza to, że SRK w obecnej formie znajduje się pomiędzy dwoma modelami:

- modelem regulacyjnym, który powinien zapewniać stabilność i uniwersalność,
- oraz modelem operacyjnym, który wymaga aktualności i szczegółowości.

Brak jednoznacznego rozstrzygnięcia tej relacji prowadzi do sytuacji, w której dokument realizuje te funkcje w sposób nie w pełni zrównoważony. Szczególnie istotnym wnioskiem wynikającym z analizy jest to, że cyberbezpieczeństwo jako dziedzina wiedzy i praktyki operacyjnej jest ograniczone w przypadku stosowania wyłącznie liniowego modelu kwalifikacji. Wymaga ono podejścia uwzględniającego:

- wielowymiarowość kompetencji,
- ich specjalizację,
- oraz dynamiczny charakter ich rozwoju.

W konsekwencji SRK powinna być postrzegana nie jako statyczny dokument opisujący aktualny stan wiedzy, lecz jako narzędzie systemowe wspierające rozwój kompetencji w dłuższej perspektywie czasowej.

Istotnym elementem wniosków jest również ocena potencjału wdrożeniowego dokumentu. W obecnym kształcie jego zastosowanie w praktyce może być częściowo ograniczone bez dodatkowych mechanizmów interpretacyjnych, szczególnie w środowiskach operacyjnych, takich

jak SOC, CSIRT czy zespoły DevSecOps, gdzie kluczowe znaczenie ma szybkie i jednoznaczne mapowanie kompetencji na role i zadania. Brak takiego powiązania w SRK powoduje, że jej wykorzystanie w procesach zarządzania zasobami ludzkimi, planowania szkoleń czy oceny kompetencji może być utrudnione.

Jednocześnie należy podkreślić, że identyfikowane ograniczenia nie przekreślają wartości projektu jako całości. Przeciwnie – wskazują one na kierunki jego dalszego rozwoju oraz potencjał przekształcenia w narzędzie o wysokiej użyteczności systemowej. Warunkiem tego jest jednak wprowadzenie zmian o charakterze strukturalnym, a nie jedynie redakcyjnym.

Kluczowe znaczenie ma tu dalsze rozwijanie modelu:

- kompetencyjnego (zamiast narzędziowego),
- adaptacyjnego (zamiast statycznego),
- oraz modułowego (uzupełniającego model liniowy).

Dopiero połączenie tych trzech elementów pozwala na stworzenie ramy kwalifikacji, która:

- zachowuje trwałość w czasie,
- odpowiada na zmieniające się potrzeby rynku,
- oraz znajduje realne zastosowanie w organizacjach.

Z perspektywy systemu kwalifikacji szczególne znaczenie ma zapewnienie równowagi pomiędzy szczegółowością opisu kompetencji a ich trwałością i uniwersalnością. Nadmierne powiązanie z aktualnymi rozwiązaniami technologicznymi może ograniczać możliwość długoterminowego wykorzystania SRK oraz jej interoperacyjność z innymi ramami kwalifikacji. Tak przeprojektowana SRK może stać się nie tylko dokumentem regulacyjnym, lecz rzeczywistym narzędziem wspierającym rozwój kompetencji w jednym z kluczowych sektorów współczesnej gospodarki cyfrowej.

Podsumowując, projekt sektorowej ramy kwalifikacji w cyberbezpieczeństwie należy traktować jako solidną podstawę do dalszych prac, wymagającą jednak ukierunkowanej korekty metodologicznej. W szczególności konieczne jest przesunięcie ciężaru z opisu technologii na opis zdolności, z modelu statycznego na model adaptacyjny oraz z podejścia liniowego na podejście modułowe.

7. KONKLUZJA EKSPERCKA

Przeprowadzona analiza projektu sektorowej ramy kwalifikacji w sektorze cyberbezpieczeństwa prowadzi do jednoznacznego wniosku, że stanowi on inicjatywę o wysokim znaczeniu systemowym, odpowiadającą na rzeczywiste potrzeby rozwoju kompetencji w jednym z kluczowych obszarów współczesnej gospodarki cyfrowej. Projekt ten tworzy solidną podstawę do budowy spójnego systemu kwalifikacji, zdolnego do integracji edukacji, rynku pracy oraz praktyki operacyjnej.

Jednocześnie jego obecna konstrukcja ujawnia istotne ograniczenia o charakterze metodologicznym i strukturalnym, wymagające dalszego doprecyzowania. W szczególności

odnoszą się one do nadmiernej operacjonalizacji kompetencji, częściowego niedostosowania do dynamiki środowiska zagrożeń, ograniczonego powiązania z rolami zawodowymi oraz niewystarczającej elastyczności struktury. Wyzwania te ograniczają zarówno trwałość dokumentu, jak i jego praktyczną użyteczność.

Z perspektywy eksperckiej kluczowe znaczenie ma zatem przeformułowanie podejścia przyjętego w SRK. Celowe jest dalsze ukierunkowanie dokumentu w stronę narzędzia systemowego o charakterze długoterminowym, wykraczającego poza opis aktualnych rozwiązań technicznych, wspierające rozwój kompetencji w warunkach zmienności i niepewności.

W szczególności zasadne jest:

- dalsze wzmocnienie podejścia kompetencyjnego względem podejścia narzędziowego,
- wprowadzenie mechanizmów adaptacyjnych umożliwiających systematyczną aktualizację SRK,
- oraz rozwój architektury modułowej, odzwierciedlającej rzeczywiste obszary cyberbezpieczeństwa.

Dopiero implementacja tych zmian pozwoli na uzyskanie pełnej funkcjonalności SRK jako narzędzia wspierającego rozwój kompetencji, zarządzanie zasobami ludzkimi oraz budowę zdolności organizacji do reagowania na zagrożenia.

W obecnym kształcie projekt należy zatem ocenić jako: trafny koncepcyjnie, lecz wymagający ukierunkowanej korekty metodologicznej, **w szczególności w zakresie poziomu szczegółowości oraz struktury kompetencyjnej, aby mógł w pełni realizować funkcję trwałej i operacyjnie użytecznej ramy kwalifikacji.**

Rama kwalifikacji w niebezpieczeństwie powinna nie tylko odzwierciedlać aktualny stan wiedzy i praktyki, lecz także wspierać przygotowanie do działania w warunkach zmienności i niepewności technologicznej.

Niniejsza opinia została przygotowana z udziałem wybitnego eksperta w tej dziedzinie Pana dr inż. Jerzego Stanika Profesora Wojskowej Akademii Technicznej, zastępca dyrektora Instytutu Systemów Informatycznych na Wydziale Cybernetyki.

Łączę wyrazy szacunku,

Iwona Wendel
Wiceprezes Zarządu KIGC