UZASADNIENIE

Projektowane rozporządzenie Ministra Edukacji w sprawie Sektorowej Ramy Kwalifikacji w sektorze cyberbezpieczeństwa, stanowi wykonanie upoważnienia ustawowego zawartego w art. 11 ust. 4 i 5 ustawy z dnia 22 grudnia 2015 r. o Zintegrowanym Systemie Kwalifikacji (Dz. U. z 2024 r. poz. 1606), zwanej dalej „ustawą".

W ustawie ustanowiono Polską Ramę Kwalifikacji, zwaną dalej „PRK". W PRK wyróżnia się 8 poziomów określonych przez ogólne charakterystyki efektów uczenia się. PRK ma służyć do klasyfikowania kwalifikacji włączonych do Zintegrowanego Systemu Kwalifikacji, zwanego dalej „ZSK", według poziomów, co umożliwi porównywanie kwalifikacji z różnych dziedzin w kraju i za granicą. Ustawa przewiduje tworzenie Sektorowych Ram Kwalifikacji, zwanych dalej „SRK". Zgodnie z art. 2 pkt 19 ustawy SRK stanowią opis poziomów kwalifikacji funkcjonujących w danym sektorze lub branży. Poziomy SRK odpowiadają odpowiednim poziomom PRK. SRK są więc rozwinięciem PRK pod kątem potrzeb określonych sektorów. SRK mają stanowić swoisty „pomost" między charakterystykami I i II stopnia PRK, w szczególności typowymi dla kwalifikacji o charakterze zawodowym a opisami poszczególnych kwalifikacji funkcjonujących w danym sektorze. Zgodnie z art. 11 ustawy, SRK mogą być włączone do ZSK, na wniosek ministra właściwego, w drodze rozporządzenia wydanego przez ministra właściwego do spraw oświaty i wychowania.

Główne cele włączenia SRK w sektorze cyberbezpieczeństwa do ZSK to przede wszystkim:

1) uporządkowanie kompetencji specyficznych dla sektora zgodnie ze stopniem ich złożoności, w podziale na wiedzę, umiejętności i kompetencje społeczne;
2) możliwość odpowiedniego kształtowania systemu kwalifikacji i zawodów dla potrzeb sektora cyberbezpieczeństwa, zgodnie z ZSK;
3) możliwość ocenienia stopnia złożoności kwalifikacji w sektorze;
4) umożliwienie porównywania różnych zawodów i kwalifikacji, w tym poszczególnych zbiorów zestawów efektów uczenia się, pod względem zaawansowania kompetencji, jakie należy potwierdzić, aby zdobyć daną kwalifikację albo zawód;
5) możliwość porównywania zawodów i kwalifikacji dotyczących różnych obszarów działalności w danym sektorze, do poziomów zgodnych z PRK.

Pismem z dnia 27 marca 2025 r. Minister Cyfryzacji wystąpił do Ministra Edukacji z wnioskiem dotyczącym SRK w sektorze cyberbezpieczeństwa.

W trakcie prac nad projektem SKR w sektorze cyberbezpieczeństwa wypracowano następującą definicję sektora: cyberbezpieczeństwo obejmuje podmioty/organizacje/osoby prowadzące działania w celu ochrony systemów informacyjnych, usług, produktów oraz użytkowników i innych podmiotów przed cyberzagrożeniami dla zapewnienia ich niezakłóconego funkcjonowania. Przy czym przez cyberzagrożenia rozumie się wszelkie potencjalne okoliczności, zdarzenia lub działania, które mogą wyrządzić szkodę w systemach, usługach, produktach, spowodować zakłócenia w nich lub w inny sposób niekorzystnie wpłynąć na nie oraz ich interesariuszy. Przez działania w celu ochrony systemów, usług i produktów rozumie się czynności wykonywane na etapach identyfikacji, ochrony, wykrywania, reakcji, odbudowy procesu cyberbezpieczeństwa oraz audytu. Działania te są realizowane zarówno podczas wdrażania systemu, usługi lub produktu, ich eksploatacji, jak i wycofania tego systemu, usługi lub produktu z użytkowania. Przez system informacyjny rozumie się strukturę obejmującą komponenty techniczne i organizacyjne, pozwalającą na przetwarzanie informacji.

Rodzajami działalności gospodarczej, które odpowiadają wskazanym procesom, według rozporządzenia Rady Ministrów z dnia 18 grudnia 2024 r. w sprawie Polskiej Klasyfikacji Działalności (PKD) (Dz. U. poz. 1936), są trzy działy PKD 2025:

1) sekcja K – Działalność usługowa w zakresie telekomunikacji, programowania komputerowego, doradztwa, infrastruktury obliczeniowej oraz pozostała działalność usługowa w zakresie informacji Dział 62 – Działalność związana z programowaniem, doradztwem w zakresie informatyki i działalności powiązane;

2) Sekcja N – Działalność profesjonalna, naukowa i techniczna Dział 70.22.Z Doradztwo w zakresie prowadzenia działalności gospodarczej i pozostałe doradztwo w zakresie Zarządzania;

3) Sekcja Q – Edukacja Dział 85.59.D Pozostałe pozaszkolne formy edukacji, gdzie indziej niesklasyfikowane.

Za pomocą SRK w sektorze cyberbezpieczeństwa pracodawcy mogą szerzej spojrzeć na kompetencje branżowe występujące w swoim środowisku biznesowym, a dzięki temu efektywniej zarządzać zasobami ludzkimi i skuteczniej konkurować na rynku pracy. Do największych zalet wynikających z korzystania z tego narzędzia zalicza się wsparcie w procesach analizy luk kompetencyjnych branży czy firmy, planowania rozwoju zasobów ludzkich oraz siatki płacowej ich stanowisk, a także rekrutacji i selekcji personelu.

W oparciu o SRK w sektorze cyberbezpieczeństwa szkoły i placówki systemu oświaty mogą dostosowywać realizowane programy nauczania do aktualnych i realnych potrzeb rynku pracy. Oznacza to, że tabela kompetencji wspiera te podmioty przy poszerzaniu i modyfikacji realizowanych programów nauczania oraz uzupełnianiu luk kompetencyjnych uczniów, np. dotyczących umiejętności praktycznych czy miękkich. Dodatkowo może być przydatna w doradztwie zawodowym dla uczniów czy monitorowaniu sukcesów absolwentów szkół.

SRK w sektorze cyberbezpieczeństwa jest narzędziem, które wspiera uczelnie w dopasowaniu programów kierunku studiów do bieżących trendów w rozwoju branży. Dzięki temu studenci mogą być lepiej przygotowani do wejścia na rynek pracy i osiągnięcia sukcesu zawodowego. Tabele kompetencji umożliwiają także monitorowanie postępów studentów oraz ocenę efektywności programów kierunków studiów.

Firmy szkoleniowe, przy wykorzystaniu SRK w cyberbezpieczeństwie, mogą skutecznie projektować specjalistyczne szkolenia, dzięki czemu są w stanie przygotować ofertę szytą na miarę potrzeb konkretnej branży oraz oczekiwań swoich klientów. Przy pomocy SRK mogą wybierać poszczególne kompetencje i dobierać je do efektów danego programu szkoleniowego. Mogą także przygotowywać egzaminy weryfikujące zdobytą wiedzę, umiejętności oraz kompetencje społeczne. Dzięki gradacji złożoności kompetencji w SRK w cyberbezpieczeństwie łatwiej im również przygotowywać ofertę szkoleniową z podziałem na różne poziomy zaawansowania.

Na podstawie art. 91 pkt 5 oraz art. 11 ust. 3 pkt 6 ustawy, w związku z wnioskiem Ministra Cyfryzacji z dnia 6 marca 2024 r., Rada Interesariuszy ZSK w dniu 14 listopada 2024 r. pozytywnie zaopiniowała celowość włączenia SKR w sektorze cyberbezpieczeństwa do ZSK oraz jej zgodność z PRK.

Rozporządzenie określa charakterystyki efektów uczenia w podziale na wiedzę, umiejętności i kompetencje społeczne dla poziomów SRK w sektorze cyberbezpieczeństwa obejmujące sześć poziomów odpowiadających poziomom 3–8 PRK.

SRK w sektorze cyberbezpieczeństwa została podzielona na 9 wyznaczników, które stanowią obszary kluczowe:

I. Wstępne wymagania dla cyberbezpieczeństwa

II. Identyfikacja

III. Ochrona

IV. Wykrywanie

V. Reakcja

VI. Odbudowa

VII. Audyt cyberbezpieczeństwa w ramach zarządzania bezpieczeństwem

VIII. Standardy pracy

IX. Komunikacja i współpraca.

W projekcie rozporządzenia w ramach poszczególnych kategorii SRK zostały zawarte kompetencje odnoszące się do:

1) cyberbezpieczeństwa, które należy rozumieć jako działania, polityki i procedury mające na celu utrzymanie ciągłości działania organizacji przez ochronę systemów, sieci, danych, ich użytkowników oraz innych podmiotów przed nieautoryzowanym dostępem, wykorzystaniem, ujawnieniem, zakłóceniem, modyfikacją lub zniszczeniem oraz zdolność do odzyskiwania ciągłości działania po incydencie;
2) danych, tj. zarejestrowane, przetwarzane i przesyłane przez nadawcę w formie komunikatu fakty, które nie są uporządkowane, przetworzone ani połączone zgodnie z celem i zadaniami odbiorcy;
3) systemu, tj. układu współpracujących ze sobą dwóch składowych: sprzętu komputerowego (hardware) oraz oprogramowania (software) w celu osiągnięcia założonego celu. Na system składa się kilka warstw: sprzętowa, system operacyjny, programy narzędziowe, programy użytkowe oraz wykorzystujący go użytkownicy;
4) IACS, tj. model odnoszący się do urządzeń automatyki przemysłowej i systemów sterowania (ang. Industrial Automation and Control Systems);
5) obiektu, tj. terminu w kontekście cyberbezpieczeństwa, który może odnosić się do różnych koncepcji i aspektów. W zależności od kontekstu, obiekt w cyberbezpieczeństwie może mieć następujące znaczenia:
   a) obiekt danych – w kontekście ochrony danych i prywatności obiektem może być zbiór informacji, dokument lub plik, który zawiera wrażliwe dane, takie jak dane osobowe klientów lub tajemnice handlowe. Obiekty danych są ważnym celem ochrony przed cyberatakami i naruszeniami danych,
   b) obiekt ataku – w dziedzinie cyberbezpieczeństwa obiekt ataku oznacza cel, na którym atakujący próbuje przeprowadzić atak lub naruszenie. To może być konkretny system komputerowy, sieć, aplikacja lub urządzenie,

c) obiekt monitoringu – w kontekście monitoringu bezpieczeństwa obiektami monitoringu mogą być konkretne zasoby lub aktywności w systemie informatycznym, które są śledzone w celu wykrycia nieprawidłowości lub podejrzanej aktywności (np. obiektem monitoringu może być ruch sieciowy, logi zdarzeń czy zmiany w konfiguracji systemu),

d) obiekt kontroli dostępu – w zarządzaniu dostępem i kontroli dostępu do zasobów informatycznych obiektem może być użytkownik, aplikacja lub urządzenie, które próbuje uzyskać dostęp do określonych zasobów. Systemy bezpieczeństwa mogą oceniać, czy dany obiekt ma uprawnienia do dostępu do określonych zasobów i czy jest to autoryzowane,

e) obiekt analizy – w analizie zagrożeń i reagowaniu na incydenty obiektem analizy mogą być dane, logi lub ślady, które są badane w celu zrozumienia natury ataku lub incydentu. To może obejmować analizę kodu złośliwego, wykrywanie anomalii w ruchu sieciowym itp.,

f) obiekt zarządzania ryzykiem – w zarządzaniu ryzykiem w dziedzinie cyberbezpieczeństwa obiektami są czynniki ryzyka, które mogą wpływać na bezpieczeństwo organizacji. To mogą być systemy, aplikacje, osoby, procesy czy technologie, które są oceniane pod kątem potencjalnych zagrożeń i skutków incydentów;

6) sieci, czyli połączenia urządzeń w celu wymiany danych między nimi. Urządzenia komunikują się ze sobą za pomocą mediów transmisyjnych, wykorzystując odpowiednie protokoły komunikacyjne;

7) modelu OSI, tj. standardu opisującego strukturę komunikacji w sieci teleinformatycznej w podziale na siedem warstw abstrakcji, takich jak: fizyczna, łącze danych, sieć, transport, sesja, prezentacja i aplikacja. Pełna nazwa: ISO OSI RM (ang. International Organization for Standardization Open Systems Interconnection Reference Model);

8) IoT (ang. Internet of Things), tj. koncepcji wykorzystywania urządzeń niebędących typowymi komputerami (na przykład elektroniki użytkowej w gospodarstwach domowych) do budowy sieci urządzeń gromadzących i przetwarzających dane oraz komunikujących się ze sobą za pomocą sieci komputerowej lub innej;

9) skryptu, czyli krótkiego programu komputerowego lub zestawu instrukcji, który jest używany do wykonywania określonych działań lub zadań w środowisku informatycznym. Skrypt może być używany zarówno w celach bezpieczeństwa, jak i w innych aspektach

zarządzania systemem lub automatyzacji procesów. Co do zasady skrypt nie jest kompilowany i nie wymaga się go do działania;

10) programowania, czyli procesu tworzenia i rozwijania programów komputerowych przez formułowanie instrukcji, które komputer może zrozumieć i wykonywać. Programowanie jest fundamentalnym elementem informatyki i polega na tworzeniu algorytmów, czyli sekwencji logicznych kroków, które określają, jakie działania ma wykonać komputer;
11) aplikacji webowych, czyli programów uruchamianych w przeglądarce, które przez zaprojektowany interfejs mają dostarczać użytkownikowi konkretną usługę udostępnianą przez serwer;
12) aplikacji mobilnych, czyli programów instalowanych i uruchamianych na urządzeniach przenośnych (mobilnych), np. smartfonach, tabletach. Jest to publicznie dostępne oprogramowanie z interfejsem dotykowym, zaprojektowane do wykorzystania na urządzeniach mobilnych;
13) aplikacji desktopowych, czyli programów, które są instalowane i uruchamiane bezpośrednio na urządzeniu, np. komputerze stacjonarnym, laptopie, tablecie, smartfonie. Do ich działania nie jest konieczny dostęp do internetu;
14) incydentów, tj. zdarzeń lub zespołów niepożądanych lub niespodziewanych zdarzeń związanych z cybezpieczeństwem, które stwarzają znaczne prawdopodobieństwo zakłóceń działań biznesowych;
15) SOC, tj. całodobowa usługa (24/7/365) składającą się z pracy systemów teleinformatycznych oraz ekspertów do spraw bezpieczeństwa. Pozwala ona wynajętym specjalistom na analizowanie zasobów teleinformatycznych pod kątem ich bezpieczeństwa oraz reagowanie na ewentualnie pojawiające się incydenty;
16) anomalii, tj. zachowań (zdarzeń) niezgodnych z procedurami, standardami przyjętymi w organizacji;
17) środowiska, czyli ogół warunków funkcjonowania danego podmiotu w przestrzeni przetwarzania i wymiany informacji tworzonej przez systemy teleinformatyczne wraz z powiązaniami między nimi oraz relacjami z użytkownikami, scharakteryzowany przez wyzwania (szanse i ryzyka) oraz zagrożenia dla osiągania przyjętych celów;
18) identyfikacji, tj. przygotowanie i wdrożenie odpowiednich działań w celu zidentyfikowania i oceny wystąpienia ryzyk wpływających na cyberbezpieczeństwo;
19) łańcucha dostaw, tj. sieci podmiotów zaangażowanych w tworzenie, dystrybucję i sprzedaż produktów lub usług. Obejmuje wszystkie etapy procesu, począwszy od pozyskania

surowców, przez produkcję, magazynowanie, transport i sprzedaż, aż do dostarczenia produktu do ostatecznego odbiorcy;

20) bazy CMDB, tj. baza danych zarządzania konfiguracją (ang. Configuration Management Database) – baza danych zawierająca informacje o aktywach oraz relacjach między nimi;
21) usługi katalogowej, czyli usługi będącej specjalizowaną bazą danych, pozwalającą na przechowywanie, przetwarzanie i odwzorowywanie relacji między obiektami obecnymi w usłudze katalogowej, którymi są użytkownicy, aplikacje, komputery, serwery i inne urządzenia komputerowe. Usługi katalogowe pozwalają na budowanie hierarchicznych grup obiektów, ułatwiają zarządzanie nimi (np. zarządzanie uprawnieniami poszczególnych grup). Jednym z najpopularniejszych standardów usług katalogowych jest ITU-T X.500, implementowany jako protokół LDAP (ang. Lightweight Directory Access Protocol). Jednym z najpopularniejszych komercyjnych rozwiązań usługi katalogowej jest Active Directory;
22) podatności, tj. słabości aktywów lub zabezpieczenia, która może być wykorzystana przez zagrożenia rozumiane jako potencjalna przyczyna niepożądanego incydentu mogącego wywołać szkodę w systemie lub organizacji;
23) ochrony, tj. przygotowania i wdrożenia odpowiednich zabezpieczeń w celu zapewnienia poprawnego świadczenia usług i działania produktów;
24) uwierzytelniania, tj. weryfikacja tożsamości osoby, aplikacji lub systemu. Jest to sprawdzenie, czy podmiot, który próbuje uzyskać dostęp, jest tym, za kogo się podaje. Proces uwierzytelniania może obejmować używanie haseł, certyfikatów, biometrycznych danych (takich jak odciski palców lub rozpoznawanie twarzy) albo innych metod;
25) systemu IT, tj. systemu komputerowego, sieci i oprogramowania służącego do przetwarzania informacji. Składają się one zazwyczaj z komputera lub komputerów połączonych siecią, oprogramowania oraz urządzeń peryferyjnych: drukarek, skanerów, myszki, klawiatury itp.;
26) SaaS, tj. oprogramowania jako usługi (ang. Software as a Service) – jeden z modeli, obok IaaS i PaaS, usługi przetwarzania w chmurze. Dostawca usługi hostuje oprogramowanie klienta;
27) IaaS, tj. infrastruktury jako usługi (ang. Infrastructure as a Service) – jeden z modeli, obok SaaS (ang. Software as a Service) i PaaS (ang. Platforma as a Service), usługi przetwarzania w chmurze, w którym zasoby obliczeniowe są hostowane w chmurze.

Dostawca usługi hostuje fizyczną infrastrukturę, oprogramowanie oraz sieć o określonej przepustowości;

28) PaaS, tj. platformy jako usługi (ang. Platform as a Service) – jeden z modeli, obok IaaS i SaaS, usługi przetwarzania w chmurze, w którym dostawca udostępnia platformę programistyczną lub developerską;
29) systemu OT (Operational Technology), tj. wszelkie urządzenia i systemy (software) służące do zarządzania i monitorowania pracy w środowiskach produkcyjnych i przemysłowych. Ich głównym zadaniem jest wspomaganie mające na celu poprawę wydajności produkcji i bezpieczeństwa operacyjnego;
30) szkodliwego oprogramowania, znanego również jako malware (rodzaj oprogramowania stworzonego z zamiarem wyrządzenia szkód, kradzieży informacji lub przeprowadzenia innych nielegalnych działań na komputerze, sieci lub urządzeniach. Szkodliwe oprogramowanie jest tworzone przez cyberprzestępców w celu osiągnięcia korzyści finansowych, szkodzenia innym lub pozyskiwania poufnych danych;
31) autoryzacji, tj. procesu weryfikacji uprawnień użytkownika lub systemu, aby określić, czy dana osoba, aplikacja lub urządzenie ma prawo dostępu do określonych zasobów lub funkcji systemu informatycznego. Autoryzacja jest jednym z kluczowych elementów kontroli dostępu i ma na celu zapewnienie, że tylko uprawnione osoby lub systemy uzyskują dostęp do zasobów lub danych, które są im przydzielone;
32) zdarzenia, czyli zachowania w systemach informatycznych, np. logowanie do komputera. Może mieć charakter zgodny z procedurami, standardami lub niezgodny. W drugim wypadku mówimy o anomalii;
33) wykrywania, tj. przygotowania i wdrożenie odpowiednich działań w celu zidentyfikowania wystąpienia zdarzeń wpływających na cyberbezpieczeństwo;
34) ataku SQL Injection, tj. ataku polegającego na wykorzystaniu błędów programistycznych, głównie w językach skryptowych (PHP, ASP itd.). Błędy te polegają na braku filtrowania danych wejściowych, które są wykorzystywane do dynamicznie generowanych zapytań SQL i przez co możliwa jest zmiana całości lub fragmentu zapytania do systemu bazodanowego. Wykorzystanie podatności aplikacji na ataki wstrzyknięcia kodu SQL może doprowadzić do ujawnienia zawartości bazy danych lub jej modyfikacji;
35) ataku XSS (ang. Cross Site Scripting), tj. ataku polegającego na wstrzyknięciu do przeglądarki użytkownika fragmentu kodu JavaScript bądź innego języka skryptowego, który może być uruchomiony w przeglądarce. W efekcie atakujący ma możliwość

wykonania dowolnego kodu skryptowego w przeglądarce, co pozwala na wykradzenie ciasteczek sesyjnych użytkownika, a w konsekwencji przechwyceniem całej jego sesji;

36) SSRF, tj. podatności SSRF (ang. Server-Side Request Forgery) występującej, gdy aplikacja internetowa pobiera dane z zewnętrznych zasobów bez walidacji adresu URL podanego przez użytkownika. Pozwala to wymusić na aplikacji wysłanie spreparowanego requestu (żądania) do nieoczekiwanego miejsca docelowego, nawet gdy znajduje się ono w sieci lokalnej lub jest zabezpieczone VPN, firewallem lub ma aktywną listę ACL;
37) SSTI, tj. podatności umożliwiającej zdalne wykonanie kodu przez przygotowanie odpowiednio spreparowanego wejścia (payload) z wykorzystaniem natywnej składni specyficznej dla wykorzystanego silnika szablonów;
38) testu penetracyjnego, tj. testu bezpieczeństwa systemu informatycznego, którego celem jest wykrycie podatności (słabości) tego systemu przez próbę odzworowania działań, które mogą być wykonywane przez atakującego podczas rzeczywistego ataku komputerowego. Testy penetracyjne mogą być prowadzone manualnie przez testera lub w sposób częściowo zautomatyzowany i wykorzystują gotowe lub specjalnie przygotowane exploity, tj. metody wykorzystania podatności obecnych w systemach komputerowych celem wykonania pożądanego przez atakującego działania, najczęściej wykonania programu przygotowanego przez atakującego lub zwiększenia jego uprawnień. Cechą charakterystyczną testów penetracyjnych jest nie tylko poprzestanie na wyszukiwaniu podatności, ale próba ich wykorzystania (sprawdzenia, czy da się „włamać" do systemu). Testy penetracyjne mogą obejmować działania w postaci testów bezpieczeństwa fizycznego (dostania się przez testującego do obszaru chronionego kontrolą dostępu, np. chronionego budynku), a także działań socjotechnicznych;
39) OWASP, tj. dokumentu organizacji OWASP zawierającego 10 najistotniejszych podatności dla aplikacji webowych. Dokument jest regularnie aktualizowany;
40) ataku XXE, tj. ataku przeprowadzanego w momencie parsowania dokumentu XML dostarczonego z zewnętrznego źródła. Jest to atak podobny do SQL Injection, ponieważ ma miejsce w momencie przetwarzania XML zawierającego referencje do zewnętrznych źródeł, które zostaną załadowane do treści XML;
41) API, tj. interfejsu programowania, czyli zestawu reguł, protokołów i narzędzi używanych do budowy i interakcji z oprogramowaniem i aplikacjami. Definiuje on sposób, w jaki aplikacje lub moduły systemów powinny się ze sobą komunikować, określa dostępne do użycia funkcje, zasady ich działania oraz wskazuje dane niezbędne do ich wykonania. Określa również reguły umożliwiające bezpieczne przesyłanie danych, np. przez

wdrażanie uwierzytelniania (weryfikację tożsamości użytkownika) oraz autoryzację (nadanie uprawnień);

42) dekompilacji, tj. procesu tłumaczenia pliku wykonywalnego do wyższego rzędu (kod źródłowy);
43) inżynierii odwrotnej/inżynierii wstecznej (ang. reverse engineering), tj. ogółu czynności prowadzących do odzyskania ze skompilowanego kodu maszynowego (dostępnego zazwyczaj w formie plików wykonywalnych analizowanych programów) instrukcji stanowiących kod źródłowy. Inżynieria wsteczna pozwala także na odtworzenie i ustalenie wymagań oraz przyjętych rozwiązań projektowych badanego oprogramowania, wykonywanych operacji, wykorzystywanych protokołów komunikacyjnych i zastosowanych algorytmów. Inżynieria wsteczna może być prowadzona w celu audytu bezpieczeństwa analizowanych aplikacji, wyeliminowania zabezpieczeń zastosowanych przez twórców oprogramowania (np. blokady kopiowania, sprawdzania aktywacji systemu) lub próbie stworzenia własnego rozwiązania na podstawie cudzej pracy. Inżynieria wsteczna może dotyczyć też urządzeń (np. sprzętu komputerowego) i protokołów komunikacyjnych;
44) skanowania, tj. działania, które po zbadaniu portów, adresów IP, hostów oraz sieci pozwala zidentyfikować aktywne urządzenia, rozpoznać uruchomione serwisy oraz systemy operacyjne i dostarczyć informacji o zaistniałych zdarzeniach, np. powstałych lukach w zabezpieczeniach czy potencjalnych zagrożeniach. Skanowanie pomaga również rozpoznać topologię sieci i konfigurację urządzeń dostępowych oraz wskazać otwarte porty;
45) adresu IP, tj. adresu, który umożliwia urządzeniom, które znajdują się w tych samych lub różnych sieciach, komunikowanie się ze sobą. Adresy IPv4 to adresy 32-bitowe, reprezentowane w notacji dziesiętnej z kropkami, np. 192.168.1.0. Adresy IPv6 są adresami 128-bitowymi, reprezentowanymi w notacji szesnastkowej z dwukropkami, np. 2a01:612f:1047:9710:e9e0:ca9a:586b:dd04. Istnieją dwie metody przydzielania adresów IP w interfejsie sieciowym: dynamiczne i statyczne. Dynamiczne adresy są przydzielane przez serwer DHCP z dostępnej puli adresów, a statyczne adresy IP są przypisywane ręcznie;
46) buffer overflow, tj. podatności polegającej na próbie zapisu większej ilości danych do bufora pamięci, przekraczająca jego rozmiar;
47) formatu string, tj. działania polegającego na wykorzystaniu błędnego sposobu przekazywania argumentów do funkcji operujących na ciągach znaków. Ich celem jest

napisanie i zastosowanie takiego programu, który przez wykorzystanie błędnego sposobu przekazywania argumentów umożliwia wklejenie łańcucha znaków w odpowiednim polu tak, aby przemycić niebezpieczny kod do źle zabezpieczonej aplikacji;

48) kodu źródłowego, tj. szczegółowych instrukcji pisanych przez programistę i zrozumiałych dla programisty przy wykorzystaniu danego języka programowania, których wykonanie przez komputer prowadzi do prezentacji wyników operacji na dostępnych danych;
49) sieci AIM, tj. części systemów zautomatyzowanego zarządzania infrastrukturą AIM, czyli rozwiązania udostępniającego funkcje ilustrowania, zarządzania, analizy i planowania;
50) socjotechniki, tj. czynności wywierania wpływu na ludzi, praktyczne zastosowanie podstępu przez stosowanie środków psychologicznych i metod manipulacji mających na celu wyłudzenie określonych informacji bądź nakłonienie do realizacji określonych działań. Celem takiego działania jest nieautoryzowane pozyskanie poufnych lub niedostępnych w inny sposób informacji. Podstawowe metody socjotechniki to np. perswazja, manipulacja, intensyfikacja lęku;
51) exploit, tj. gotowych narzędzi, udostępnianych zazwyczaj w formie skryptu lub kodu źródłowego, służących do wykorzystania określonej podatności;
52) redteamingu, tj. ogółu działań podejmowanych przez zespół (ang. red team), którego celem jest zasymulowanie ataku na określoną organizację lub część jej struktury. Red teaming ma na celu sprawdzenie poziomu bezpieczeństwa organizacji i prawidłowego działania jej systemów zabezpieczeń, zarówno informatycznych (np. systemy antywirusowe, zapobiegania wyciekom danych, zapory sieciowe), technicznych (systemy kontroli dostępu, monitoringu wizyjnego), jak i organizacyjnych (odpowiednio przygotowane, wdrożone i przestrzegane polityki i procedury bezpieczeństwa). Red teaming wykorzystuje metody znane z testów penetracyjnych, testów bezpieczeństwa fizycznego i testów socjotechnicznych, ale nie ogranicza się do ich zakresu, będąc zazwyczaj działaniem bardziej rozciągniętym w czasie, zakresie i wykorzystywanych technikach od testów penetracyjnych. Zazwyczaj celem red teamingu jest uzyskanie dostępu do określonego zasobu (np. wykradnięcie jakichś informacji) lub dotarcie do miejsca objętego kontrolą dostępu;
53) reakcji, tj. przygotowania i wdrożenia odpowiednich działań mających na celu reakcję i odpowiedź na wykryte zdarzenie związane z cyberbezpieczeństwem. Jest to działanie krótkoterminowe i doraźne;
54) materiału dowodowego, tj. materiału, który może pomóc w rekonstrukcji ataków, identyfikacji luk w zabezpieczeniach i świadczeniu dowodów w celu identyfikacji

sprawców lub dowiedzenia popełnionych działań nieautoryzowanych. Materiał dowodowy ulotny w obszarze cyberbezpieczeństwa odnosi się do informacji lub śladów, które mogą istnieć tylko przez krótki czas. Przykładem są tymczasowe pliki logów, sesje połączeń sieciowych, dane w pamięci podręcznej, które mogą zawierać ważne informacje na temat ataków lub działań nieautoryzowanych. Ze względu na swoją nietrwałość, zbieranie i analiza tych materiałów ulotnych są kluczowe dla zrozumienia ataków i podejmowania odpowiednich działań naprawczych. Materiał dowodowy nieulotny w obszarze cyberbezpieczeństwa to taki, który jest trwały i może istnieć przez dłuższy czas. Obejmuje np. kopie zapasowe danych, zrzuty stanu systemów, archiwalne pliki logów oraz nagrania zdarzeń związanych z bezpieczeństwem;

55) nośnika danych, tj. urządzenia wykorzystywanego do gromadzenia, przechowywania, przetwarzania i transmisji danych. Nośniki mogą być wewnętrzne (np. dyski twarde) oraz zewnętrzne/przenośne (np. pendrive, karta pamięci, dysk zewnętrzny czy płyta CD);
56) odbudowy, tj. analizy zdarzenia, przygotowania i wdrożenia odpowiednich działań mających na celu realizację planów na wypadek sytuacji kryzysowych oraz przywrócenia funkcji lub usług, które zostały zakłócone w wyniku zdarzenia związanego z cyberbezpieczeństwem;
57) kopii bezpieczeństwa, tj. zestawu danych, które w przypadku ich utracenia (np. ataku wirusa, przypadkowego usunięcia) pozwolą na odtworzenie oryginalnych danych;
58) umowy SLA (ang. Service Level Agreement), tj. umowy o gwarantowanym poziomie świadczenia usług, określającej, na jakim minimalnym poziomie dostawca będzie świadczyć określone usługi klientowi. Przez „umowę OLA" (ang. Operational Level Agreement) rozumie się umowę, która określa zobowiązania wewnętrzne między operacyjnymi jednostkami zapewniającymi poziom świadczenia usług. Celem tego kontraktu jest zagwarantowanie poziomu usług ustalonego w OLA, głównie utrzymania i rozwoju;
59) branży, tj. jednego z obszarów dla poszczególnych sektorów, np. branży ciepłowniczej (sektor energetyczny), branży suplementów (sektor farmeceutyczny);
60) kwalifikacji dokumentów (ang. Design Qualification), tj. weryfikacji dokumentacji projektowej, podwykonawczej oraz instrukcji eksploatacyjnych obiektu pod kątem zgodności zawartych w nich wymagań ze stanem faktycznym;
61) kwalifikacji instalacyjnej (IQ ang. Installation Qualification), tj. udokumentowanego sprawdzenia i potwierdzenia, że zainstalowane lub zmodyfikowane urządzenie,

oprogramowanie lub system są zgodne z zatwierdzonym projektem, zaleceniami producenta lub wymaganiami użytkownika;

62) kwalifikacji procesu (Działania) (PQ ang. Performance Qualification), tj. udokumentowanego sprawdzenia i potwierdzenia, że urządzenia i instalacje pomocnicze, połączone w jedną funkcjonalną całość, mogą pracować efektywnie i powtarzalnie zgodnie z zatwierdzoną metodą prowadzenia procesu i specyfikacjami.

Poszczególnym składnikom opisu SRK zostały przypisane kody. Ma to na celu ułatwienie posługiwania się nią między innymi w trakcie odnoszenia efektów uczenia się przewidzianych dla kwalifikacji.

Proponuje się, aby rozporządzenie weszło w życie po upływie 14 dni od dnia ogłoszenia.

Projekt rozporządzenia nie zawiera przepisów technicznych w rozumieniu rozporządzenia Rady Ministrów z dnia 23 grudnia 2002 r. w sprawie sposobu funkcjonowania krajowego systemu notyfikacji norm i aktów prawnych (Dz. U. poz. 2039, z późn. zm.) i w związku z tym nie podlegało notyfikacji.

Projektowane rozporządzenie nie jest sprzeczne z prawem Unii Europejskiej.

Projektowane rozporządzenie nie wymaga przedstawienia właściwym organom i instytucjom Unii Europejskiej, w tym Europejskiemu Bankowi Centralnemu, w celu uzyskania opinii, dokonania powiadomienia, konsultacji albo uzgodnienia.

Projektowane rozporządzenie nie podlega ocenie w zakresie oceny skutków regulacji w trybie § 32 uchwały nr 190 Rady Ministrów z dnia 29 października 2013 r. – Regulamin pracy Rady Ministrów (M.P. z 2026 r. poz. 404).

Projekt rozporządzenia nie ma wpływu na działalność mikroprzedsiębiorców, małych i średnich przedsiębiorców w rozumieniu ustawy z dnia 6 marca 2018 r. – Prawo przedsiębiorców (Dz. U. z 2025 r. poz. 1480, z późn. zm.).

Odnosząc się do § 12 pkt 1 załącznika do rozporządzenia Prezesa Rady Ministrów z dnia 20 czerwca 2002 r. w sprawie „Zasad techniki prawodawczej” (Dz. U. z 2026 r. poz. 300) należy stwierdzić, że projekt rozporządzenia uwzględnia regulacje, w stosunku do których nie ma możliwości, aby mogły być podjęte za pomocą alternatywnych środków.