W celu ułatwienia wypełniania w Zintegrowanym Rejestrze Kwalifikacji elektronicznego formularza „Wniosku o włączenie kwalifikacji do ZSK" zapraszamy zainteresowane podmioty do zapoznania się z formularzem pomocniczym do przygotowania wniosku o włączenie kwalifikacji rynkowej do ZSK. Jest on wzorowany na elektronicznym formularzu wniosku o włączenie kwalifikacji do ZSK, który musi wypełnić wnioskodawca w systemie informatycznym Zintegrowanego Rejestru Kwalifikacji. Formularz umożliwia zapoznanie się z treścią i strukturą docelowego formularza w ZRK. Jest w pełni edytowalny, co pozwala na przygotowanie w nim wszystkich wymaganych treści, a następnie ich przekopiowanie do elektronicznego formularza w systemie informatycznym ZRK. Przy czym należy pamiętać, że niemożliwe jest automatyczne zaciągnięcie informacji z formularza pomocniczego do formularza w ZRK – należy je każdorazowo skopiować do odpowiedniego pola w formularzu ZRK.

Formularz pomocniczy
do przygotowania wniosku o włączenie kwalifikacji rynkowej do ZSK,

opracowany na podstawie ustawy z dnia 22 grudnia 2015 r. o Zintegrowanym Systemie Kwalifikacji[1] oraz elektronicznego formularza „Wniosek o włączenie kwalifikacji do ZSK" w ZRK

TYP FORMULARZA W ZRK: Wniosek o włączenie kwalifikacji do ZSK

I. INFORMACJE OGÓLNE O KWALIFIKACJI

1. Nazwa kwalifikacji*

Pole obowiązkowe Art. 15 ust. 1 pkt 2a)
Należy wpisać pełną nazwę kwalifikacji, która ma być widoczna w ZRK i być umieszczana na dokumencie potwierdzającym jej uzyskanie. Nazwa kwalifikacji (na ile to możliwe) powinna:
- jednoznacznie identyfikować kwalifikację,
- różnić się od nazw innych kwalifikacji,
- różnić się od nazwy zawodu, stanowiska pracy, tytułu zawodowego, uprawnienia,
- być możliwie krótka,
- nie zawierać skrótów,
- być oparta na rzeczowniku odczasownikowym (np. gromadzenie, przechowywanie, szycie).

Maksymalna liczba znaków: 300

Obsługa incydentów cyberbezpieczeństwa

2. Skrót nazwy

[1] Tekst jednolity, Dziennik Ustaw RP z 16 listopada 2018 r., poz. 2153, z późniejszymi zmianami

Pole nieobowiązkowe. Pole wprowadzone w celu zapewnienia przejrzystości informacji gromadzonych w ZRK. Uwaga: jeżeli nazwa kwalifikacji nie ma skrótu pole należy pozostawić puste!

Maksymalna liczba znaków: 150

3. Rodzaj kwalifikacji*

Wskazanie, czy kwalifikacja jest: kwalifikacją pełną, czy kwalifikacją cząstkową. Należy wskazać, że kwalifikacja jest cząstkowa.

Kwalifikacja cząstkowa

4. Proponowany poziom Polskiej Ramy Kwalifikacji*

Pole obowiązkowe Art. 15 ust. 1 pkt 4.
Należy wpisać swoją propozycję poziomu PRK. Ostatecznie poziom PRK nada minister.

4 PRK

5. Krótka charakterystyka kwalifikacji, obejmująca informacje o działaniach lub zadaniach, które potrafi wykonywać osoba posiadająca tę kwalifikację oraz orientacyjny koszt uzyskania dokumentu potwierdzającego otrzymanie danej kwalifikacji*

Pole obowiązkowe Art. 15 ust. 1 pkt 2d) oraz pkt 5.
Należy podać wybrane informacje o kwalifikacji skierowane do osób zainteresowanych uzyskaniem kwalifikacji oraz do pracodawców, które pozwolą im szybko ocenić, czy dana kwalifikacja jest właśnie tą, której poszukują.
Ponadto należy podać orientacyjną wysokość opłaty za przeprowadzenie walidacji i wystawienie dokumentu potwierdzającego otrzymanie danej kwalifikacji.

Maksymalna liczba znaków: 4000

Osoba posiadająca kwalifikację „Obsługa incydentów cyberbezpieczeństwa" jest przygotowana do wykonywania zadań związanych z obsługą zdarzeń będących incydentami naruszającymi cyberbezpieczeństwo. Osoba posiadająca kwalifikacje rozpoznaje zdarzenia, które są incydentami naruszającymi cyberbezpieczeństwo oraz gromadzi dane dotyczące incydentów, niezbędne do dokonania zgłoszenia do właściwego podmiotu Krajowego Systemu Cyberbezpieczeństwa. Ustala moment wystąpienia incydentu, czas jego trwania, przebieg oraz ustala zadania, procesy, zasoby i osoby, na które ma wpływ zaistniałe naruszenie. Identyfikuje skutki wystąpienia określonego incydentu cyberbezpieczeństwa oraz rozpoznaje incydenty krytyczne wymagające natychmiastowej reakcji. Przygotowuje i wysyła zgłoszenie o zaistniałym incydencie cyberbezpieczeństwa do właściwego podmiotu. Koordynuje działania związane z obsługą incydentu, w szczególności ustala działania oraz zasoby wymagane do ich zrealizowania. Monitoruje stopień realizacji działań związanych z obsługą incydentu przez inne osoby i podmioty, w szczególności ocenia ich skuteczność oraz wskazuje kryteria zakończenia obsługi incydentu. Osoba posiadająca kwalifikację przygotowana jest również do wykonywania zadań związanych z poinformowaniem osób i podmiotów, których dotyczy naruszenie bezpieczeństwa.

Orientacyjna wysokość opłaty za przeprowadzenie walidacji i wystawienie dokumentu potwierdzającego otrzymanie danej kwalifikacji: 3.000,00 zł (trzy tysiące złotych).

6. Orientacyjny nakład pracy potrzebny do uzyskania kwalifikacji [godz.]*

Uwaga: Pole sumuje się automatycznie po wypełnieniu pól dotyczących zestawów efektów uczenia się.

7. Grupy osób, które mogą być zainteresowane uzyskaniem kwalifikacji*

Pole obowiązkowe Art. 15 ust. 1 pkt 2f)
Należy podać informacje na temat grup osób, które mogą być szczególnie zainteresowane uzyskaniem danej kwalifikacji (np. osoby zarządzające nieruchomościami, specjaliści z zakresu telekomunikacji, osoby powracające na rynek pracy itp.).

Maksymalna liczba znaków: 4000

Kwalifikacja kierowana jest do osób odpowiedzialnych za funkcjonowanie systemów informatycznych w organizacjach mających obowiązek zgłaszania, do odpowiedniego podmiotu Krajowego Systemu Cyberbezpieczeństwa, incydentów cyberbezpieczeństwa, administratorów sieci i systemów informatycznych oraz osób odpowiedzialnych za komunikowanie się z podmiotami Krajowego Systemu Cyberbezpieczeństwa.

7a. Należy zaznaczyć poniższe pole jeśli dotyczy (pole wprowadzone od 1.09.2019 r.)

☐ **Kwalifikacja może być przydatna dla uczniów szkół branżowych lub techników kształcących się w określonych zawodach** Rozporządzenie MEN z dnia 16 maja 2019 r.

W szkole prowadzącej kształcenie zawodowe kształcenie odbywa się w oparciu o podstawy programowe określone w rozporządzeniu MEN z dnia 16 maja 2019 r. w sprawie podstaw programowych kształcenia w zawodach szkolnictwa branżowego oraz dodatkowych umiejętności zawodowych w zakresie wybranych zawodów szkolnictwa branżowego (Dz. U. poz. 991). Część godzin zajęć może zostać przeznaczona na realizację obowiązkowych zajęć edukacyjnych przygotowujących uczniów do uzyskania kwalifikacji rynkowej funkcjonującej w ZSK, związanej z nauczanym zawodem (§ 4 ust 5 pkt 2 rozporządzenia Ministra Edukacji Narodowej z dnia 3 kwietnia 2019 r. w sprawie ramowych planów nauczania dla publicznych szkół (Dz. U. poz. 639)).
Należy wskazać zawody (zgodnie z klasyfikacją zawodów szkolnictwa branżowego określoną w załączniku nr 2 do rozporządzenia Ministra Edukacji Narodowej z dnia 15 lutego 2019 r. w sprawie ogólnych celów i zadań kształcenia w zawodach szkolnictwa branżowego oraz klasyfikacji zawodów szkolnictwa branżowego (Dz. U. poz. 316)), w przypadku których zasadne jest przygotowywanie uczniów do uzyskania kwalifikacji rynkowej objętej wnioskiem.

7b. Wskazanie zawodów szkolnictwa zawodowego, z którymi związana jest kwalifikacja

Jeżeli w punkcie 7a wskazano przydatność kwalifikacji, to z rozwijanej listy branż i zawodów należy wybrać te zawody, z którymi związana jest wnioskowana kwalifikacja.

8. Wymagane kwalifikacje poprzedzające

Pole nieobowiązkowe.
Jeżeli są wymagane konkretne kwalifikacje pełne lub cząstkowe, które musi posiadać osoba ubiegająca się o nadanie kwalifikacji (np. dyplom ukończenia studiów medycznych albo dyplom potwierdzający kwalifikacje zawodowe w zawodzie np. „technik rachunkowości" albo świadectwo potwierdzające kwalifikację w zawodzie np. „naprawa zegarów i zegarków" itp.), należy je wpisać.

Maksymalna liczba znaków: 2000

Nie dotyczy

9. W razie potrzeby warunki, jakie musi spełniać osoba przystępująca do walidacji*

Pole obowiązkowe Art. 15 ust.1 pkt 2g)
O ile dotyczy, należy podać warunki, które musi spełniać osoba, żeby przystąpić do walidacji i móc uzyskać kwalifikację (np. wymagany poziom wykształcenia – wyższe, podstawowe itp.; zaświadczenie o niekaralności; orzeczenie lekarskie o braku przeciwwskazań itp.)
Warunki przystąpienia do walidacji określone w opisie kwalifikacji powinny być możliwe do zweryfikowania (warunki te nie są tożsame z warunkami zatrudnienia).

Kompetencje wynikające z doświadczenia zawodowego powinny być odzwierciedlone przede wszystkim w opisie efektów uczenia się wymaganych dla kwalifikacji. Dlatego doświadczenie zawodowe powinno być wskazywane jako warunek przystąpienia do walidacji, jedynie w szczególnie uzasadnionych przypadkach.
Jeżeli nie ma takich warunków należy wpisać: „Nie dotyczy".

Maksymalna liczba znaków: 25000

Nie dotyczy

10. Zapotrzebowanie na kwalifikację*

Pole obowiązkowe Art. 15 ust.1 pkt 2i)
Należy wskazać, na jakie aktualne lub przewidywane potrzeby społeczne i gospodarcze (regionalne, krajowe, europejskie) odpowiada kwalifikacja. Warto odwołać się do różnych źródeł np. opinii organizacji gospodarczych, trendów obserwowanych na rynku pracy, prognoz dotyczących rozwoju technologii, a także strategii rozwoju kraju lub regionu.

Maksymalna liczba znaków: 25000

„Obsługa incydentów cyberbezpieczeństwa" to kwalifikacja, na którą zapotrzebowanie występuje nie tylko w sektorze IT, ale też, z uwagi na powszechność rozwiązań cyfrowych, wśród przedsiębiorstw większości działów gospodarki narodowej.

Digitalizacja jest uznawana za jedną z fundamentalnych i najdynamiczniej zachodzących zmian społecznych i ekonomicznych w XXI wieku. Powszechnie rozumiany jest również istotny wpływ digitalizacji na możliwości rozwojowe gospodarki narodowej jako części globalnego obiegu ekonomicznego. Mimo świadomości tego faktu i ciągłego rozwoju potencjału cyfrowego gospodarki, w Polsce od lat utrzymuje się dość duża luka technologiczna. Według opublikowanego w roku 2016 raportu „Cyfrowa Polska", wiele sektorów gospodarki (m.in. produkcja przemysłowa, transport i logistyka, energetyka oraz usługi komunalne) z powodu niskiego poziomu nasycenia technologiami cyfrowymi nie osiągały swojego całkowitego potencjału, zaś najsilniej scyfryzowany wówczas sektor finansowy odnotowywał aż 13 procentową lukę technologiczną w porównaniu do państw Europy Zachodniej [1]. Obecnie, według raportu „DIGI INDEX 2022 Poziom digitalizacji produkcji w Polsce", prezentującego wyniki badania wykonanego w okresie pandemii COVID-19, nadal tylko 0,7% firm deklaruje poziom cyfryzacji produkcji przekraczający 81% [2]. Wynik ten jest oparty na uśrednionych wartościach poziomu cyfryzacji dla 4 głównych branż gospodarki (Machinery, Automotive, Chemistry&Pharmacy, Food&Beverages). Największa grupa 28% badanych przedsiębiorstw plasuje się na poziomie 21-40%, zaś najwyższy stopień digitalizacji produkcji wykazują reprezentanci sektora Automotive, gdzie dla 20% badanych firm wynosi on 60-79%. DIGI INDEX podaje wskaźnik podejścia do digitalizacji gospodarki w 4-punktowej skali, przy czym wynik poniżej 2 punktów jest równoznaczny z powiększającą się luką technologiczną. Według autorów raportu, w 2022 roku właściwy dla Polski wskaźnik DIGI INDEX wzrósł z 1,8 w latach ubiegłych do 2,4 punktu. Interpretując ten wynik można uważać go za pozytywny sygnał, świadczący o tym, że większość badanych firm przeszła już przez etap przygotowań do aktywnej implementacji rozwiązań cyfrowych, głównie w zakresie procesów zarządczych i produkcyjnych. Firmy zwiększają budżety na cyfryzację, gdyż w coraz większym stopniu są przekonane o jej korzyściach. Najczęściej wskazywane są oszczędność kosztów (38,7%), wyższa wydajność (38,0%) oraz większe bezpieczeństwo produkcji i danych (27,3%).

Od jakości i szybkości transformacji cyfrowej, czyli inaczej cyfryzacji, zależą możliwości rozwojowe polskich przedsiębiorstw. Dotychczas, pomimo funkcjonowania w warunkach globalnej ekonomii rynkowej, procesy cyfryzacji zachodziły w Polsce dużo wolniej niż w innych krajach. Dotyczyły one przy tym głównie lokalnych oddziałów międzynarodowych korporacji, przedsiębiorstw wytwarzających oprogramowanie i oferujących usługi IT oraz wciąż stosunkowo nielicznych firm przemysłu 4.0 oraz startupów. Pozytywną stroną tej sytuacji jest fakt, że względne opóźnienie procesów cyfryzacji polskiej gospodarki powodowało, że wprowadzane rozwiązania były z reguły najbardziej nowoczesne, przez co analitycy postrzegali Polskę jako potencjalnego cyfrowego rywala zachodnich gospodarek, posiadającego poważny potencjał wzrostu ilościowego procesów transformacji cyfrowej, przy jednoczesnej innowacyjności stosowanych rozwiązań i wysokiej wydajności rezultatów [3].

Wspomniany wyraźny wzrost wskaźnika DIGI INDEX oraz podniesienie przez przedsiębiorstwa nakładów na cyfryzację wynika z wpływu pandemii COVID-19, której przebieg skłonił wiele firm do rozpoczęcia planowania lub realizacji procesów cyfryzacji. Pomimo pozytywnego trendu rozwojowego, wskazane opóźnienia w stosunku do państw Europy Zachodniej powodują, że Polska wciąż zajmuje w zestawieniach jedno z ostatnich miejsc, zarówno w pod względem stopnia cyfryzacji gospodarki, jak też kompetencji cyfrowych pracowników.

Poziom cyfryzacji Polski odbiega zarówno od lidera na tym polu, czyli Stanów Zjednoczonych, jak też państw Europy Zachodniej. W Stanach Zjednoczonych procesami transformacji cyfrowej objęte jest ogółem 18% gospodarki, zaś w Europy Zachodniej średnio 12%. Tymczasem w Polsce gospodarka jest scyfryzowana tylko w 8%. Stopień cyfryzacji polskich przedsiębiorstw jest wciąż średnio o około 34% niższy niż w takich państwach jak Francja, Holandia, Niemcy, Szwecja, Wielka Brytania czy Włochy [4].

Według danych Komisji Europejskiej, w 2021 roku, podobnie jak w roku 2020, w zakresie cyfryzacji gospodarki Polska uplasowała się na, 24 miejscu wśród 27 państw członkowskich Unii Europejskiej [4]. Analizy te opierają się na wskaźniku Digital Economy and Society Index (dalej: DESI), stworzonym w celu oceny poziomu ucyfrowienia gospodarek i społeczeństw państw UE. DESI za najbardziej „cyfrowe" państwa europejskie uznaje Finlandię, Szwecję, Holandię i Danię, dla których współczynnik wynosi blisko 70 na 80 możliwych do uzyskania punktów. Państwa te od lat są liderami rankingu europejskiego i jednocześnie znajdują się także w czołówce światowej, tuż za Koreą Południową, Japonią i Stanami Zjednoczonymi. W roku 2021 europejska średnia DESI wynosiła 50,7 pkt, zaś wynik Polski osiągnął 41 punktów i wyprzedzała ona takie kraje jak Grecja, Bułgaria i Rumunia, których DESI plasowały się poniżej 40 punktów. Statystyki wskazują, że mimo ogólnego odbiegania Polski od średniej UE w zakresie cyfryzacji, obecnie dwa kluczowe elementy wskaźnika DESI, łączność i cyfrowe usługi publiczne, osiągnęły już w Polsce poziom średniej. Sytuacja taka rokuje pozytywnie, gdyż wysoka dostępność cyfrowych technologii łączności i wysoki poziom cyfryzacji sektora publicznego są przykładem i motorem dla reszty gospodarki w zakresie cyfryzacji.

Polski rząd od roku 2013 dąży do stworzenia spójnego systemu rozwiązań prawno-instytucjonalnych oraz upowszechniania dobrych praktyk wspierających bezpieczeństwo cyfrowej gospodarki. Wtedy to przyjęto strategię Polityki Ochrony Cyberprzestrzeni RP, której celem strategicznym było osiągnięcie akceptowalnego poziomu bezpieczeństwa cyberprzestrzeni państwa [5]. W 2017 r. strategia ta została zastąpiona przez Krajowe Ramy Polityki

Cyberbezpieczeństwa RP. Z kolei od 2019 r. obowiązującym dokumentem jest Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019 – 2024 [6]. Jako główny cel Strategii wskazano podniesienie poziomu odporności kraju na cyberzagrożenia, w tym zwłaszcza ochrony w sektorach: publicznym, militarnym i prywatnym oraz promowanie wiedzy i dobrych praktyk wśród obywateli.

Najistotniejszym aktem prawnym ustanawiającym w Polsce system cyberbezpieczeństwa jest Ustawa z dnia 5 lipca 2018 r. o Krajowym Systemie Cyberbezpieczeństwa (Dz.U.2020.1369 t.j.), która wdraża w Polsce dyrektywę Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (Dz. Urz. UE L 194 z 19.07.2016, str. 1).

Ustawa ta stworzyła w Polsce system cechujący się jasnym przydziałem zadań i odpowiedzialności, umożliwiający sprawne działania w zakresie wykrywania, zapobiegania i minimalizowania skutków ataków naruszających cyberbezpieczeństwo RP. Obejmuje on samorządy, dostawców usług cyfrowych i większość firm będących operatorami tak zwanych usług kluczowych dla funkcjonowania społeczeństwa. Wszystkie te podmioty, zgodnie z ustawą o Krajowym Systemie Cyberbezpieczeństwa, mają obowiązek raportować incydenty do właściwego zespołu CSIRT (Computer Security Incident Response Team). Zespoły te, to współpracujące ze sobą oraz z organami właściwymi do spraw cyberbezpieczeństwa: CSIRT NASK (Naukowej i Akademickiej Sieci Komputerowej), CSIRT GOV (Agencji Bezpieczeństwa Wewnętrznego) oraz CSIRT MON resortu obrony narodowej. Razem tworzą krajowy system zarządzania ryzykiem w obszarze cyberbezpieczeństwa, który przeciwdziała zagrożeniom o charakterze ponadsektorowym i transgranicznym oraz zapewniają koordynację obsługi zgłoszonych incydentów.

Kluczowym i jednocześnie najsłabszym elementem systemu są pracownicy wykazanych w ustawie podmiotów objętych nadzorem Krajowego Systemu Cyberbezpieczeństwa, czyli samorządów, dostawców usług cyfrowych i operatorów usług kluczowych. Ich zadaniem jest obsługa incydentów naruszenia cyberbezpieczeństwa w lokalnych sieciach i systemach informatycznych. Braki kadrowe na rynku pracy IT powodują, że w wymienionych podmiotach, w tym zwłaszcza w mniejszych przedsiębiorstwach i samorządach lokalnych, często pracują osoby nie posiadające odpowiednich kompetencji pozwalających na właściwe identyfikowanie i klasyfikowanie incydentów, ocenę ich skali i możliwych skutków, nadawanie priorytetów, koordynowanie obsługi incydentów oraz komunikację z podmiotami Krajowego Systemu Cyberbezpieczeństwa, w tym zgłaszanie incydentów, i z podmiotami zewnętrznymi (np. klientami, dostawcami, regulatorami). Z uwagi na obecne w ostatnich latach napięcia międzynarodowe i związane z nimi wzmożone występowanie możliwości ataków cybernetycznych na krajową infrastrukturę i urzędy, jakość wskazanych kompetencji nabiera niezwykłej istotności dla funkcjonowania społeczeństwa i bezpieczeństwa państwa.

Mimo rosnącego zapotrzebowania, wskazane wyżej kompetencje nie są obecne w zakresie szkolnictwa branżowego, kształcącego w zawodach Technik Informatyk i Technik Programista. Efekty kształcenia w tych zawodach zawierają jedynie ogólny zapis „stosuje zasady cyberbezpieczeństwa”, który nie odnosi się do zadań pracowniczych związanych z obsługą incydentów cyberbezpieczeństwa, a jedynie do kwestii prewencji. Zagadnienia te dopiero zaczynają być

widoczne w efektach uczenia się studiów kierunków informatycznych jak również dedykowanych studiów podyplomowych.

Z kolei w obszarze edukacji pozaformalnej można zaobserwować dużo więcej ofert szkoleń pozwalających na rozwój kompetencji związanych z obsługą incydentów cyberbezpieczeństwa. Rozwój tej formy kształcenia wynika z rosnącego zainteresowania ze strony potencjalnych pracowników i pracodawców chcących pozyskać osoby o właściwych kompetencjach. Realizowane kursy i szkolenia nie zawsze jednak pozwalają na ich rzetelną walidację, zaś ich programy i zakładane efekty uczenia się mogą się bardzo różnić. Powoduje to sytuację, w której uzyskiwane zaświadczenia i certyfikaty w rzeczywistości nie zawsze oddają realny poziom umiejętności, co w negatywny sposób odbija się na jakości pracy przeszkolonych osób i może bezpośrednio wpłynąć na przebieg potencjalnych kryzysów związanych z cyberzagrożeniami.

Reasumując można stwierdzić, że braki specjalistów od obsługi incydentów cyberbezpieczeństwa wpływają na bezpieczeństwo kraju, instytucji i społeczeństwa polskiego. Rozwój form szkoleniowych w tym zakresie powinien wiązać się z odpowiednimi procedurami walidacyjnymi, które zapewni kwalifikacja „Obsługa incydentów cyberbezpieczeństwa". Warte podkreślenia jest, że stworzy ona możliwość potwierdzenia posiadanych umiejętności i kompetencji nie tylko dla osób związanych z IT. Umożliwi ona potwierdzanie kompetencji nabywanych zarówno w drodze edukacji, samokształcenia czy praktyki zawodowej. Uzyskiwany certyfikat będzie atrakcyjny zarówno dla jego posiadaczy jak i dla zatrudniających ich jednostek samorządu, instytucji i podmiotów gospodarczych, gdyż będzie w sposób obiektywny gwarantował wysoki poziom kompetencji.

Przypisy:

1. Cyfrowa Polska. Szansa na technologiczny skok do globalnej pierwszej ligi gospodarczej, McKinsey &Company 2016, https://www.mckinsey.com/pl/~/media/mckinsey/locations/europe%20and%20middle%20east/polska/raporty/cyfrowa%20polska/cyfrowa-polska.ashx [dostęp: 24.07.2022].

2. Digi Index 2022. Poziom digitalizacji produkcji w Polsce, Siemens 2022, https://new.siemens.com/pl/pl/o-firmie/raporty-siemens/digi-index-2022.html#Pobierz [dostęp: 24.07.2022].

3. J. Novak, M. Purta, T. Marciniak, K. Ignatowicz, K. Rozenbaum, K. Yearwood, The rise of Digital Challengers. How digitization can become the next growth engine for Central and Eastern Europe, raport opracowany przez McKinsey Company, 2018, https://www.mckinsey.com/~/media/McKinsey/Featured%20Insights/Europe/Central%20and%20Eastern%20Europe%20needs%20a%20new%20engine%20for%20growth/The-rise-of-Digital-Challengers.ash [dostęp: 20.07.2022].

4. Indeks gospodarki cyfrowej i społeczeństwa cyfrowego (DESI) na 2021 r. Polska, 2022, https://ec.europa.eu/newsroom/dae/redirection/document/80596 [dostęp: 20.07.2022].

5. Cyber Policy, NASK, https://cyberpolicy.nask.pl/category/strategia-cyberbezpieczenstwa-rp/ [dostęp: 24.07.2022].

6. Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019-2024, https://www.gov.pl/web/cyfryzacja/strategia-cyberbezpieczenstwa-rzeczypospolitej-polskiej-na-lata-2019-2024 [dostęp: 24.07.2022].

11. Odniesienie do kwalifikacji o zbliżonym charakterze oraz wskazanie kwalifikacji ujętych w ZRK zawierających wspólne zestawy efektów uczenia się*

Pole obowiązkowe Art. 15 ust. 1 pkt 2k)
Należy wskazać, czym kwalifikacja różni się od innych kwalifikacji o zbliżonym charakterze. Punktem odniesienia powinny być kwalifikacje funkcjonujące w ZSK. Ponadto należy wskazać kluczowe kwalifikacje wpisane do ZRK, które zawierają co najmniej jeden wspólny, kluczowy zestaw efektów uczenia się.

Maksymalna liczba znaków: 6000

Kwalifikacje o zbliżonym charakterze ujęte w ZRK:

- Zarządzanie cyberbezpieczeństwem - specjalista
- Zarządzanie cyberbezpieczeństwem - menedżer
- Zarządzanie cyberbezpieczeństwem - ekspert

Wymienione kwalifikacje obejmują umiejętności pozwalające na kompleksowe zarządzanie cyberbezpieczeństwem. Przeznaczone są one przede wszystkim dla specjalistów w zakresie cyberbezpieczeństwa odpowiedzialnych za ochronę informacji, bezpieczeństwo infrastruktury teleinformatycznej oraz kształtowanie polityki bezpieczeństwa, na różnych szczeblach organizacji.

Kwalifikacja "Obsługa incydentów cyberbezpieczeństwa" koncentruje się natomiast na wiedzy i umiejętnościach związanych z formalną obsługą incydentu w obszarze cyberbezpieczeństwa. W szczególności kwalifikacja obejmuje efekty uczenia się niezbędne do zidentyfikowania incydentu w obszarze cyberbezpieczeństwa, opisania go zgodnie z wymogami ustawy o Krajowym Systemie Cyberbezpieczeństwa oraz zgłoszenia do właściwego podmiotu. Kwalifikacja ta jest przeznaczona przede wszystkim dla osób administrujących systemami informatycznymi lub odpowiedzialnych za ich funkcjonowanie w organizacjach, które mają obowiązek zgłaszania naruszeń bezpieczeństwa do podmiotów KSC lub osób, które w tych organizacjach odpowiedzialne są za współpracę z podmiotami Krajowego Systemu Cyberbezpieczeństwa.

Kwalifikacja nie posiada wspólnych zestawów efektów uczenia się z wymienionymi powyżej kwalifikacjami o zbliżonym charakterze.

Ponadto w ZRK ujęto następujące kwalifikacje:

- Kształtowanie polityki niezawodności i cyberbezpieczeństwa w przemyśle w zakresie zasobów ludzkich i technicznych
- Zarządzanie niezawodnością i cyberbezpieczeństwem w przemyśle w zakresie zasobów ludzkich i proceduralnych
- Zarządzanie niezawodnością i cyberbezpieczeństwem w zakresie urządzeń oraz technologii w przemyśle.

Wymienione kwalifikacje dedykowane są do stosowania w przemyśle, ze szczególnym zorientowaniem na systemy informatyczne nadzorujące przebieg procesów technologicznych lub produkcyjnych SCADA (ang. Supervisory Control And Data Acquisition). Wymienione kwalifikacje koncentrują się na zagadnieniach bezpieczeństwa w środowiskach systemów sterowania przemysłowego w zakresie przemysłu procesowego. W wymienionych

kwalifikacjach nie zidentyfikowano zestawów uczenia się wspólnych dla kwalifikacji “Obsługa incydentów cyberbezpieczeństwa”.

11a. Należy zaznaczyć poniższe pole jeśli dotyczy (pole wprowadzone od 1.09.2019 r.)

☐ **Kwalifikacja zawiera wspólne lub zbliżone zestawy efektów kształcenia z „dodatkowymi umiejętnościami zawodowymi” w zakresie wybranych zawodów szkolnictwa branżowego**

Dodatkowe umiejętności zawodowe

Należy wybrać z listy „dodatkowe umiejętności zawodowe” (określone w rozporządzeniu MEN z dnia 16 maja 2019 r. w sprawie podstaw programowych kształcenia w zawodach szkolnictwa branżowego oraz dodatkowych umiejętności zawodowych w zakresie wybranych zawodów szkolnictwa branżowego, załącznik Nr 33) zawierające wspólne lub zbliżone zestawy efektów kształcenia z zestawami efektów uczenia się określonymi w kwalifikacji rynkowej.

11b. Wskazanie „dodatkowych umiejętności zawodowych” w zakresie wybranych zawodów szkolnictwa branżowego zawierających wspólne lub zbliżone zestawy efektów kształcenia (Branża – Zawód – Umiejętność)

Jeżeli w punkcie 11a udzielono pozytywnej odpowiedzi, to z rozwijanej listy branż, zawodów i dodatkowych umiejętności zawodowych należy wybrać te umiejętności, które zawierają wspólne lub zbliżone zestawy efektów kształcenia z wnioskowaną kwalifikacją.

12. Typowe możliwości wykorzystania kwalifikacji*

Pole obowiązkowe Art. 15 ust. 1 pkt 2j)
Należy wskazać przykładowe możliwości zatrudnienia i dalszego uczenia się osoby posiadającej daną kwalifikację, np.:
- Do pracy na jakich stanowiskach przygotowuje dana kwalifikacja?
- Jakie perspektywy dalszego rozwoju otwierają się dla osoby, która uzyskała tę kwalifikację?

Maksymalna liczba znaków: 4000

Osoba posiadająca kwalifikację może podjąć zatrudnienie w organizacjach posiadających obowiązek zgłaszania incydentów cyberbezpieczeństwa do podmiotów Krajowego Systemu Cyberbezpieczeństwa. Może również podjąć zatrudnienie w podmiotach prowadzących zespoły reagowania na incydenty lub monitorowania cyberbezpieczeństwa na stanowiskach wymagających kontaktu z podmiotami Krajowego Systemu Cyberbezpieczeństwa oraz w podmiotach Krajowego Systemu Cyberbezpieczeństwa.

13. Wymagania dotyczące walidacji i podmiotów przeprowadzających walidację*

Pole obowiązkowe Art. 15 ust.1 pkt 2h)
Należy podać tylko takie wymagania, które muszą obowiązywać każdą instytucję przeprowadzającą walidację, żeby zapewnić odpowiedni poziom wiarygodności i porównywalności wyników walidacji w skali całego kraju. Wskazane wymagania powinny pozwalać na tworzenie różnych scenariuszy walidacji w różnych instytucjach.
Wymagania mogą dotyczyć:
- doboru metod stosowanych w walidacji - służących weryfikacji efektów uczenia się wymaganych dla kwalifikacji, ale także (o ile to potrzebne) identyfikowaniu i dokumentowaniu efektów uczenia się;
- kompetencji osób przeprowadzających walidację;
- warunków organizacyjnych i materialnych niezbędnych do przeprowadzenia walidacji.
Odpowiednio do potrzeby wymagania te mogą dotyczyć pojedynczych efektów uczenia się i poszczególnych lub wszystkich zestawów efektów uczenia się, wymaganych dla kwalifikacji.
Należy brać pod uwagę, że spełnienie tych wymagań jest jednym z warunków uzyskania przez daną instytucję uprawnień do nadawania kwalifikacji (uzyskania statusu „instytucji certyfikującej”).
Więcej na temat walidacji: "Walidacja – nowe możliwości zdobywania kwalifikacji", IBE 2016.

Maksymalna liczba znaków: 25000

1. Etap weryfikacji

1.1. Metody

Do weryfikacji efektów uczenia się mogą być stosowane następujące metody:

- test teoretyczny**;**
- analiza dowodów i deklaracji opcjonalnie uzupełniona wywiadem swobodnym;
- obserwacja w warunkach symulowanych.

1.2. Zasoby kadrowe

Komisja walidacyjna musi składać się z co najmniej dwóch członków, w tym przewodniczącego. Przewodniczący komisji musi spełniać następujące warunki:

- posiada kwalifikację pełną z 7 poziomem PRK (dyplom ukończenia studiów II stopnia lub jednolitych studiów magisterskich);
- legitymuje się co najmniej rocznym doświadczeniem w przeprowadzaniu egzaminów w obszarze cyberbezpieczeństwa osiągniętym w okresie ostatnich 6 lat.

Członek komisji walidacyjnej musi spełniać następujące warunki:

- posiada kwalifikację pełną z 6 poziomem PRK (dyplom ukończenia studiów I stopnia);
- legitymuje się co najmniej rocznym doświadczeniem w przeprowadzaniu egzaminów w obszarze cyberbezpieczeństwa osiągniętym w okresie ostatnich 3 lat.

Ponadto, co najmniej jeden z członków komisji musi posiadać udokumentowane minimum 5-letnie doświadczenie zawodowe w obszarze cyberbezpieczeństwa.

1.3. Sposób organizacji walidacji oraz warunki organizacyjne i materialne

Walidacja może być prowadzona w trybie stacjonarnym, online lub hybrydowym.

W przypadku organizacji walidacji w trybie stacjonarnym instytucja certyfikująca musi zapewnić:

- pracownię wyposażoną w stanowisko komputerowe dla każdego uczestnika walidacji.

W przypadku organizacji walidacji w trybie online lub hybrydowym instytucja certyfikująca musi zapewnić:

- dostęp do systemu obsługi testów i egzaminów indywidualnie dla każdego uczestnika.

2. Etap identyfikowania i dokumentowania efektów uczenia się

Instytucja certyfikująca może zapewniać wsparcie dla kandydatów w zakresie identyfikowania oraz dokumentowania posiadanych efektów uczenia się. Korzystanie z tego wsparcia nie jest obowiązkowe.

Etapy identyfikowania i dokumentowania mogą być realizowane dowolnymi metodami.

14. Propozycja odniesienia do poziomu sektorowych ram kwalifikacji (o ile dotyczy)

Jeśli w danym sektorze lub branży funkcjonuje Sektorowa Rama Kwalifikacji, która jest włączona do ZSK, zgodnie z Art. 15 ust. 1 pkt 4 należy to pole wypełnić poprzez podanie nazwy odpowiedniej ramy i wpisanie swojej propozycji poziomu w tej ramie.

Maksymalna liczba znaków: 1000

Nie dotyczy

II. EFEKTY UCZENIA SIĘ WYMAGANE DLA KWALIFIKACJI

15. Syntetyczna charakterystyka efektów uczenia się*

Pole obowiązkowe Art. 15 ust. 1 pkt 3 oraz art. 9 ust. 1 pkt 1a)
Należy przedstawić w zwięzłej formie ogólną charakterystykę wiedzy, umiejętności i kompetencji społecznych poprzez określenie rodzajów działań, do których podjęcia będzie przygotowana osoba posiadająca daną kwalifikację.
Syntetyczna charakterystyka efektów uczenia się powinna nawiązywać do charakterystyki odpowiedniego poziomu PRK.
W szczególności syntetyczna charakterystyka powinna wskazać na:
- stopień przygotowania osoby posiadającej kwalifikację do samodzielnego działania,
- stopień złożoności działań, które osoba posiadająca kwalifikację może wykonywać,
- role, które osoba posiadająca kwalifikację może pełnić w grupie pracowników.

Maksymalna liczba znaków: 9000

Osoba posiadająca kwalifikację rozpoznaje zdarzenia, które są incydentami naruszającymi bezpieczeństwo oraz podejmuje działania niezbędne do dokonania zgłoszenia incydentu do właściwego podmiotu Krajowego Systemu Cyberbezpieczeństwa. Ustala moment wystąpienia incydentu, czas jego trwania, przebieg oraz ustala zadania, procesy, zasoby i osoby, na które ma wpływ zaistniałe naruszenie. Wskazuje incydenty krytyczne wymagające natychmiastowej reakcji, uwzględniając skutki ich wystąpienia. Ponadto koordynuje pracę osób i podmiotów realizujących działania naprawcze oraz minimalizujące następstwa wystąpienia incydentu. Ustala harmonogram działań, niezbędne zasoby oraz kryteria zakończenia obsługi incydentu cyberbezpieczeństwa. Przedstawia informacje niezbędne do podjęcia, przez osoby decyzyjne, decyzji o sposobie realizacji działań naprawczych, w tym wymienia utrudnienia, jakie mogą wiązać się z obsługą incydentu oraz analizuje zasadność podjęcia poszczególnych działań. Przekazuje informacje o zaistniałym incydencie osobom i podmiotom, których dotyczy naruszenie.

16. Wyodrębnione zestawy efektów uczenia się*

Wykaz zestawów efektów uczenia się wymaganych dla kwalifikacji, zawierający: numer porządkowy (1, 2, …), nazwy zestawów, orientacyjne odniesienie każdego zestawu do poziomu PRK oraz orientacyjny nakład pracy potrzebny do osiągnięcia efektów uczenia w każdym zestawie.
Nazwa zestawu powinna:

- *nawiązywać do efektów uczenia się wchodzących w skład danego zestawu lub odpowiadać specyfice wchodzących w jego skład efektów uczenia się,*
- *być możliwie krótka,*
- *nie zawierać skrótów,*
- *gdy jest to możliwe, być oparta na rzeczowniku odczasownikowym, np. „gromadzenie", „przechowywanie", „szycie".*

Maksymalna liczba znaków - nazwa zestawu: 500

1. Wykrywanie incydentów cyberbezpieczeństwa, 4 PRK, 50 godzin, rodzaj zestawu: obowiązkowy

2. Koordynowanie działań związanych z obsługą incydentów cyberbezpieczeństwa, 4 PRK, 30 godzin, rodzaj zestawu: obowiązkowy

17. Poszczególne efekty uczenia się w zestawach*

Pole obowiązkowe Art. 15 ust. 1 pkt 3) oraz art. 9 ust. 1 pkt 1c)
Należy podać poszczególne efekty uczenia się (w zestawach) opisane za pomocą umiejętności (tj. zdolności wykonywania zadań i rozwiązywania problemów) wraz z kryteriami ich weryfikacji, które doprecyzowują ich zakres oraz określają niezbędną wiedzę i kompetencje społeczne. Poszczególne efekty uczenia się (w zestawach) powinny być jednoznaczne, niebudzące wątpliwości, pozwalające na zaplanowanie i przeprowadzanie walidacji, których wyniki będą porównywalne; realne, możliwe do osiągnięcia przez osoby, dla których kwalifikacja jest przewidziana; możliwe do zweryfikowania podczas walidacji; zrozumiałe dla osób potencjalnie zainteresowanych kwalifikacją.

Podczas opisywania poszczególnych efektów uczenia się (w zestawach) korzystne jest stosowanie czasowników operacyjnych (np. wykonuje, demonstruje, diagnozuje). *Maksymalna liczba znaków – nazwa efektu uczenia się: 2000* *Maksymalna liczba znaków - kryteria weryfikacji (dla jednego efektu): 5000*	
Zestaw efektów uczenia się:	01. Wykrywanie incydentów cyberbezpieczeństwa
Efekty uczenia się* *Pole obowiązkowe Art. 15 ust. 1 pkt 3) oraz art. 9 ust. 1 pkt 1c).* *Należy podać pełną nazwę efektu uczenia się.*	**Kryteria weryfikacji*** *Pole obowiązkowe Art. 15 ust. 1 pkt 3) oraz art. 9 ust. 1 pkt 1c).* *Należy podać kryteria , na podstawie których ocenia się, czy dany efekt uczenia się został osiągnięty.*
1. Identyfikuje incydenty cyberbezpieczeństwa	a. Wyjaśnia pojęcia poufności, integralności i dostępności danych oraz systemów informatycznych; b. Wyjaśnia pojęcie incydentu cyberbezpieczeństwa; c. Charakteryzuje typy incydentów cyberbezpieczeństwa; d. Rozpoznaje zdarzenia będące incydentami cyberbezpieczeństwa; e. Określa typ incydentu według wybranej klasyfikacji, np. klasyfikacji eCSIRT.net.
2. Analizuje incydenty cyberbezpieczeństwa	a. Ustala moment wystąpienia incydentu cyberbezpieczeństwa oraz czas jego trwania na podstawie dziennika zdarzeń systemowych (logów); b. Ustala zadania, procesy, zasoby i osoby, na które wpływa incydent cyberbezpieczeństwa (na podstawie np. opisu sytuacji, dokumentacji technicznej systemu informatycznego, którego dotyczy incydent, dziennika zdarzeń systemowych); c. Opisuje przebieg incydentu cyberbezpieczeństwa (na podstawie np. opisu sytuacji, dokumentacji technicznej systemu informatycznego, którego dotyczy incydent, dziennika zdarzeń systemowych); d. Wskazuje możliwe przyczyny zaistnienia incydentu cyberbezpieczeństwa (na podstawie np. opisu sytuacji, dokumentacji technicznej systemu informatycznego, którego dotyczy incydent, dziennika zdarzeń systemowych).
3. Klasyfikuje incydenty cyberbezpieczeństwa	a. Identyfikuje skutki wystąpienia określonego incydentu cyberbezpieczeństwa; b. Szereguje incydenty cyberbezpieczeństwa według priorytetów obsługi;

	c. Wskazuje incydenty krytyczne cyberbezpieczeństwa wymagające natychmiastowej reakcji.
Zestaw efektów uczenia się:	02. Koordynowanie działań związanych z obsługą incydentów cyberbezpieczeństwa
Efekty uczenia się* *Pole obowiązkowe Art. 15 ust. 1 pkt 3) oraz art. 9 ust. 1 pkt 1c).* *Należy podać pełną nazwę efektu uczenia się.*	**Kryteria weryfikacji*** *Pole obowiązkowe Art. 15 ust. 1 pkt 3) oraz art. 9 ust. 1 pkt 1c).* *Należy podać kryteria , na podstawie których ocenia się, czy dany efekt uczenia się został osiągnięty.*
1. Wykonuje czynności związane ze zgłoszeniem incydentu cyberbezpieczeństwa	a. Wskazuje aktualne akty prawne regulujące obowiązki w zakresie zgłaszania i obsługi incydentów cyberbezpieczeństwa; b. Opisuje, wynikające z ustawy o Krajowym Systemie Cyberbezpieczeństwa oraz innych regulacji prawnych, obowiązki i procedury w zakresie zgłaszania i obsługi incydentów cyberbezpieczeństwa; c. Sporządza opis incydentu na potrzeby zgłoszenia do podmiotu Krajowego Systemu Cyberbezpieczeństwa (na podstawie np. opisu sytuacji, dokumentacji technicznej systemu informatycznego, którego dotyczy incydent, opisu technicznego incydentu, dziennika zdarzeń systemowych); d. Opisuje zasady postępowania w przypadku zaistnienia incydentów związanych z naruszeniem ochrony danych osobowych.
2. Planuje działania związane z obsługą incydentu cyberbezpieczeństwa	a. Wymienia działania niezbędne do obsługi incydentu cyberbezpieczeństwa, w tym działania naprawcze, działania ograniczające szkody; b. Przygotowuje harmonogram działań, w tym określa działania priorytetowe, działania, które mają być wykonane sekwencyjnie i te, które mogą być wykonane równolegle; c. Wskazuje zasoby techniczne i kadrowe niezbędne do obsługi incydentu cyberbezpieczeństwa; d. Wskazuje utrudnienia związane z prowadzeniem działań związanych z obsługą incydentów cyberbezpieczeństwa; e. Ocenia zasadność podjęcia działań naprawczych z uwzględnieniem ich kosztów, oczekiwanych rezultatów oraz skutków wystąpienia incydentu cyberbezpieczeństwa.

3. Planuje sposób monitorowania działań związanych z obsługą incydentu cyberbezpieczeństwa	a. Wskazuje kryteria oceny skuteczności działań związanych z obsługą incydentu cyberbezpieczeństwa ; b. Ustala kryteria zamknięcia obsługi danego incydentu cyberbezpieczeństwa; c. Formułuje wnioski dotyczące minimalizowania ryzyka jego ponownego wystąpienia na podstawie opisu przyczyn wystąpienia incydentu cyberbezpieczeństwa.
4. Charakteryzuje sposób informowania o wystąpieniu incydentu cyberbezpieczeństwa osoby i podmioty, których incydent dotyczy	a. Wskazuje grupy osób i podmiotów, które należy poinformować o zaistnieniu danego incydentu cyberbezpieczeństwa; b. Opisuje zasady informowania o incydencie cyberbezpieczeństwa, w tym związane z terminami, zakresem i stopniem szczegółowości przekazywanych informacji; c. Opisuje zagrożenia związane z przekazywaniem informacji o incydencie cyberbezpieczeństwa osobom i podmiotom, których incydent dotyczy (np. związane z wywoływaniem paniki, przekazywaniem niepełnych informacji, stratami wizerunkowymi); d. Przygotowuje komunikat dotyczący incydentu cyberbezpieczeństwa dla danej grupy odbiorców.

III. PODMIOTY

18. Wnioskodawca*
Pole obowiązkowe Art. 83 ust. 1 pkt 7 *Nazwę podmiotu wnioskującego należy wybrać z listy rozwijanej w formularzu w ZRK.*
Polskie Towarzystwo Informatyczne
19. Minister właściwy*
Pole obowiązkowe Art. 16 ust. 1 *Należy wybrać z listy nazwę ministerstwa, które zdaniem wnioskodawcy jest właściwe do rozpatrzenia wniosku.*
Minister Cyfryzacji

IV. POZOSTAŁE INFORMACJE

20. Okres ważności dokumentu potwierdzającego nadanie kwalifikacji i warunki przedłużenia jego ważności*

Pole obowiązkowe Art. 15 ust. 1 pkt 2b)
W przypadku kwalifikacji nadawanej na czas nieokreślony, należy wpisać: „Kwalifikacja ważna bezterminowo".
W przypadku kwalifikacji nadawanej na czas określony, należy podać, po jakim czasie konieczne jest odnowienie ważności oraz warunki przedłużenia ważności dokumentu potwierdzającego nadanie kwalifikacji.

Maksymalna liczba znaków: 2000

Certyfikat jest ważny 3 lata. Przedłużenie ważności certyfikatu następuje na podstawie dokumentów potwierdzających wykonywanie, w okresie ważności certyfikatu, zadań związanych z obsługą incydentów cyberbezpieczeństwa przez okres co najmniej 12 miesięcy.

21. Nazwa dokumentu potwierdzającego nadanie kwalifikacji*

Pole obowiązkowe Art. 15 ust. 1 pkt 2b)
Z rozwijanej listy należy wybrać nazwę dokumentu np. dyplom, świadectwo, certyfikat, zaświadczenie.

Certyfikat

22. Uprawnienia związane z posiadaniem kwalifikacji*

Pole obowiązkowe Art. 15 ust. 1 pkt 2e)
Należy podać, o jakie uprawnienia może się ubiegać osoba po uzyskaniu kwalifikacji.
Jeśli z uzyskaniem kwalifikacji nie wiąże się uzyskanie uprawnień, należy wpisać: „Nie dotyczy".

Maksymalna liczba znaków: 2500

Nie dotyczy

23. Kod dziedziny kształcenia*

Pole obowiązkowe Art. 15 ust. 1 pkt. 6.
Należy wpisać kod dziedziny kształcenia, o którym mowa w przepisach wydanych na podstawie art. 40 ust. 2 ustawy z dnia 29 czerwca 1995 r. o statystyce publicznej (Dz. U. z 2012 r. poz. 591, z późn. zm.).

481 - Informatyka

24. Kod PKD*

Pole obowiązkowe Art. 15 ust. 1 pkt 7.
Należy wpisać kod Polskiej Klasyfikacji Działalności (PKD), o którym mowa w Rozporządzeniu Rady Ministrów z dn. 24 grudnia 2007 r. w sprawie Polskiej Klasyfikacji Działalności (PKD) (Dz.U. 251, poz.1885, z późn. zm.).

62 - DZIAŁALNOŚĆ ZWIĄZANA Z OPROGRAMOWANIEM I DORADZTWEM W ZAKRESIE INFORMATYKI ORAZ DZIALALNOŚĆ POWIĄZANA

Uwaga:
*Pola oznaczone * to pola obowiązkowe do wypełnienia zgodnie z ustawą z dnia 22 grudnia 2015 r. o Zintegrowanym Systemie Kwalifikacji (t.j., Dziennik Ustaw RP z 16 listopada 2018 r., poz. 2153, z późniejszymi zmianami).*