„ZŁOTA SETKA”

Analiza możliwości wdrożenia programu

Ministerstwo Cyfryzacji

Warszawa, grudzień 2018 r.

Spis treści

1. Kontekst programu „Złota setka”

Program „Złota setka” ma za zadanie odpowiadać na wyzwania związane z zagrożeniami w zakresie bezpieczeństwa informatycznego państwa. W realiach XXI wieku konieczność ochrony zasobów informatycznych - cyberbezpieczeństwa kraju staje się jednym z kluczowych problemów bezpieczeństwa na poziomie administracji.

Cyberbezpieczeństwo rozumie się jako bezpieczeństwo informacji oraz tradycyjne bezpieczeństwo infrastruktury teleinformatycznej. Cyberbezpieczeństwo obejmuje ochronę zasobów informacyjnych poprzez zarządzanie ryzykami związanymi z przetwarzaniem, przechowywaniem i transferowaniem danych w systemach informatycznych.

Unia Europejska Unia Europejska podaje następującą definicję: Cyberbezpieczeństwo ogólnie odnosi się do zabezpieczeń i działań, które mogą być wykorzystywane do ochrony infrastruktury cyfrowej, zarówno cywilnej, jak i wojskowej, przed tymi zagrożeniami, które mogą dotyczyć jej warstwy sieciowej i fizycznej lub uszkodzić jej niezależność. Bezpieczeństwo cybernetyczne polega na działaniach mających na celu zachowanie dostępności i integralności sieci i infrastruktury informatycznej oraz zachowanie poufności zawartych w nich danych[1].

Poziom zagrożeń związanych z infrastrukturą teleinformatyczną rośnie wraz ze wzrostem znaczenia tej infrastruktury dla społeczeństwa, administracji i biznesu. Konieczność stałej poprawy cyberbezpieczeństwa na skalę globalna wynika z trzech głównych czynników: zwiększającej się dostępności i roli połączeń szerokopasmowych, coraz bardziej istotnej roli IT w biznesie i społeczeństwie oraz społecznej stratyfikacji umiejętności w zakresie IT[2]. W odpowiedzi na wzrost zagrożenia cyberprzestępczością oraz zmian zachodzących w społeczeństwie wiele rządów i instytucji podejmuje inicjatywy w dziedzinie cyberbezpieczeństwa polegające na opracowaniu wytycznych, wprowadzeniu standaryzacji i odpowiednich przepisów prawa i regulacji[3].

W ciągu ostatnich lat kluczowym wyzwaniem dla tradycyjnego bezpieczeństwa w administracji stał się błyskawiczny wzrost zagrożenia związanego z cyberprzestępczością oraz wojną w cyberprzestrzeni. Charakter występujących naruszeń bezpieczeństwa ciągle ewoluuje. Obecnie miejsce ataków zorientowanych na wykorzystanie słabych punktów zabezpieczeń przeprowadzanych przez indywidualnych przestępców zajęły ataki, za którymi często stoi zorganizowana przestępczość lub wrogie działania innych państw[4].

Oficjalne źródła oraz raporty branżowe wyraźnie wskazują na wzrost cyberprzestępczości oraz liczby powiązanych z nią ataków. Zgodnie z raportem „ENTERPRISE FILE SHARING AND MANAGEMENT: ACHIEVING PRODUCTIVITY AND SECURITY” w latach 2010 -2013 rocznie dochodziło do ponad 600 poważnych naruszeń tajemnicy w samych tylko Stanach Zjednoczonych[5]. Zgodnie z raportem Grand Theft Data 2015, opublikowanym przez Intel Security[6] oraz danymi Heimdal Security dane osobowe

[1] Komisja Europejska, „Wspólny komunikat do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów — Strategia bezpieczeństwa cybernetycznego Unii Europejskiej: otwarta, bezpieczna i chroniona cyberprzestrzeń”, Bruksela, 2 lipca 2013 r., s. 3, http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=1667

[2] Wdrożenie cyberbezpieczenstwa w Europie: Przegląd. ISACA, 2014r.

[3] Tamże

[4] Tamże

[5] “ENTERPRISE FILE SHARING AND MANAGEMENT: ACHIEVING PRODUCTIVITY AND SECURITY” Hanover Research z 10.2014r.

[6] https://www.mcafee.com/it/resources/reports/rp-data-exfiltration.pdf

klientów i pracowników były głównym celem ataków (62%). Rynkowa wartość danych osobowych znacząco przewyższa wartość danych kart kredytowych i płatniczych. Zgodnie z danymi Data Breach Index, z baz danych wykradane jest obecnie 6 258 450 rekordów dziennie[7], a w ciągu ostatnich 2 lat wielkość ta uległa podwojeniu, w stosunku do roku 2017 wzrost liczby incydentów wyniósł 72%.

28 sierpnia 2018r. weszła w życie ustawa o krajowym systemie cyberbezpieczeństwa implementująca europejską dyrektywę NIS (Network and Information Systems Directive, z sierpnia 2016 r.) dotyczącą bezpieczeństwa sieci i informacji. Dyrektywa NIS jest pierwszym ogólnounijnym aktem prawnym w zakresie cyberbezpieczeństwa, a zawarte w niej regulacje mają na celu zagwarantowanie równego poziomu zabezpieczeń sieci i systemów w całej Unii Europejskiej oraz wzmocnienie ochrony państw członkowskich przed cyberatakami[8].

Dokument „Krajowe Ramy Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017-2022" wskazuje między innymi cele w zakresie bezpieczeństwa teleinformatycznego oraz metody zapobiegania i reagowania w odniesieniu do incydentów oraz przywracania stanu normalnego zakłóconego incydentem, w tym zasady współpracy pomiędzy sektorami publicznym i prywatnym[9]. W ramach celu szczegółowego nr 3 - Zwiększanie potencjału narodowego oraz kompetencji w zakresie bezpieczeństwa w cyberprzestrzeni wskazano na konieczność opracowania programu pozwalającego na utrzymanie i promowanie najlepiej wykwalifikowanych specjalistów z obszaru IT i bezpieczeństwa teleinformatycznego, zatrudnionych w administracji publicznej – „Złota setka". Celem programu jest zatrzymanie w administracji publicznej pracowników o wysokich kompetencjach oraz zwiększenie ich motywacji i zaangażowania szczególnie w kontekście poważnych incydentów w systemach teleinformatycznych administracji rządowej. Poprzez poważny incydent rozumie się incydent lub grupę incydentów, które powodują lub mogą spowodować znaczną szkodę dla bezpieczeństwa publicznego, interesów międzynarodowych RP, w tym interesów gospodarczych, poziomu zaufania do instytucji publicznych, swobód obywatelskich lub zdrowia obywateli RP[10].

[7] https://breachlevelindex.com/
[8] https://home.kpmg.com/pl/pl/home/media/press-releases/2018/08/newsflash-nowe-obowiazki-firm-zwiazane-z-ustawa-o-krajowym-systemie-cyberbezpieczenstwa.html
[9] Krajowe Ramy Polityki Krajowe Ramy Polityki Krajowe Ramy Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017-2022, Ministerstwo Cyfryzacji, 2017r.
[10] Tamże.

2. Koncepcja programu

Program „Złota Setka” będzie wieloletnim programem stypendialnym. Dodatkowe wynagrodzenie będzie wypłacane z budżetu państwa za pośrednictwem Ministerstwa Cyfryzacji jako dysponenta środków dla pracowników innych urzędów centralnych.

Wynagrodzenie będzie miało formę stypendium, przy czym formuła ta wymaga dopracowania od strony prawnej, gdyż obecnie brak jest odpowiednika programu w praktyce funkcjonowania administracji w Polsce. Proponowany okres przyznawania stypendium to 4 lata.

Kandydatów do stypendiów będą zgłaszać Kierownicy Jednostek w ramach konkursów ogłaszanych przez Ministra właściwego ds. informatyzacji. Minister właściwy do spraw informatyzacji będzie ogłaszać konkursy zgodnie z umocowaniem ustawowym i wydanym przez siebie rozporządzeniem. Zasady naboru kandydatów w sposób ogólny zostaną wskazane w ramach rozporządzenia natomiast szczegółowe zasady i kryteria naboru kandydatów będą określane w regulaminie konkursu (jeśli zajdzie taka konieczność również w ramach rozporządzenia). Każdy z konkursów będzie określać liczbę stypendystów oraz ich strukturę (liczbę miejsc w ramach poszczególnych specjalizacji branżowych w obszarze cyberbezpieczeństwa). Proponowane specjalizacje oraz wstępne szacunki zapotrzebowania w ramach poszczególnych specjalizacji przedstawiono w dalszej części niniejszego opracowania. Wydaje się, że w pierwszym okresie należy zorganizować 2 lub 3 konkursy, w ramach których pierwszy stanowiłby swoisty pilotaż pozwalający na określenie rzeczywistego poziomu i możliwości rekrutacji (spełnienia kryteriów) w ramach pracowników administracji publicznej. W kolejnych latach programu organizowany byłby jeden konkurs rocznie pozwalający na uzupełnienie grona specjalistów najbardziej potrzebnych dla zapewnienia cyberbezpieczeństwa kraju.

Ministerstwo Cyfryzacji będzie zarządzać programem i jego budżetem. Szacowany poziom budżetu to od 5,5 do 10,1 miliona złotych rocznie. Szczegółowe szacunki potrzeb w zakresie finansowania przedstawiono w dalszej części dokumentu.

Zawody/specjalizacje IT objęte programem zostały wybrane na podstawie analizy specjalizacji wykorzystywanych przez firmy rekrutacyjne w Polsce. Na podstawie opisów specjalizacji oraz wiedzy eksperckiej została przygotowana lista wymagań dla kandydatów na stypendystów (w tym certyfikaty, jakimi powinni się legitymować).

Specjaliści uczestniczący w programie będą mieli obowiązek wspierania administracji rządowej (MC i innych jednostek administracji rządowej do szczebla województwa włącznie) w przypadku poważnych incydentów w systemach teleinformatycznych administracji rządowej. Problemem wymagającym rozstrzygnięcia jest prawna możliwość delegacji stypendystów do prac w innych podmiotach. Na bazie obowiązującego prawa możliwości takie są bardzo ograniczone.

Program powinien mieć charakter programu wieloletniego – optymalnie 4-letniego aby zrealizować cel długoletniego związania objętych nim specjalistów z pracą w administracji. Należy przyjąć, że z każdym ze stypendystów zawarta zostanie umowa na okres 4 lat. Takie rozwiązanie pozwoli zatrzymać odpływ kadr w okresie obowiązywania umów. Cały program powinien mieć charakter wieloletni obejmujący okres co najmniej 7 lat. W ramach takiego programu pierwszy rok pozwoliłby na stworzenie podstawowej grupy specjalistów, z którymi zawarto by umowy na kolejne 4 lata, a w kolejnych 2 przeprowadzono by kolejne 2 konkursy uzupełniające zasoby o najbardziej potrzebne specjalizacje. W kolejnych latach również zawierano by umowy 4 letnie ze stypendystami stąd perspektywa czasowa

programu powinna obejmować co najmniej 3 lata rekrutacji oraz 4 kolejne lata funkcjonowania programu.

Proponowany schemat działania programu „Złota Setka” przedstawiono na rysunku poniżej.

Rysunek 1. Schemat tworzenia i funkcjonowania programu „Złota Setka”

Źródło: opracowanie własne

Proponowane rozwiązanie opiera się przede wszystkim na procedurze konkursowej organizowanej przez Ministerstwo Cyfryzacji oraz długoletniej perspektywie funkcjonowania programu. Zaproponowany sposób organizacji pozwoli, w opinii ekspertów, na uzyskanie oczekiwanych efektów programu i realizacji celów wskazanych w dokumencie „Krajowe Ramy Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017-2022”. Długoletnie rozwiązanie i możliwości swobodnego kształtowania kryteriów szczegółowych w ramach konkursów są niezbędne na obecnym etapie ze względu na brak wiedzy w zakresie rzeczywistych zasobów kadrowych specjalistów cyberbezpieczeństwa, jakimi dysponuje administracja w Polsce. Jednocześnie rekomendujemy prace nad stworzeniem kompleksowej bazy specjalistów oraz kompetencji pracowników administracji w zakresie cyberbezpieczeństwa, co w przyszłości pozwoli na sprawniejsze planowanie i organizację zarówno programu „Złota Setka” jak i działań operacyjnych związanych z zachowanie bezpieczeństwa sieci.

3. Wytypowanie obszarów kompetencji specjalistów uczestniczących w programie

Założenia programu Złota Setka bazują na dokumencie „Krajowe Ramy Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017-2022". Zamierzeniem niniejszej Strategii jest określenie ramowych działań, mających na celu uzyskanie wysokiego poziomu odporności krajowych systemów teleinformatycznych, operatorów usług kluczowych, operatorów infrastruktury krytycznej, dostawców usług cyfrowych oraz administracji publicznej na incydenty w cyberprzestrzeni. Jak również wskazany został w strategii niezbędny kierunkowy rozwój gwarantujący silniejszą pozycję polskich podmiotów na rynku światowym. Proponowane kierunki strategiczne mają również wpływać na zwiększenie skuteczności organów ścigania i wymiaru sprawiedliwości w wykrywaniu i zwalczaniu przestępstw oraz działań o charakterze terrorystycznym i szpiegowskim w cyberprzestrzeni.

Cele wskazane w ramach „Krajowych Ram Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017-2022" określają między innymi potrzeby w zakresie:

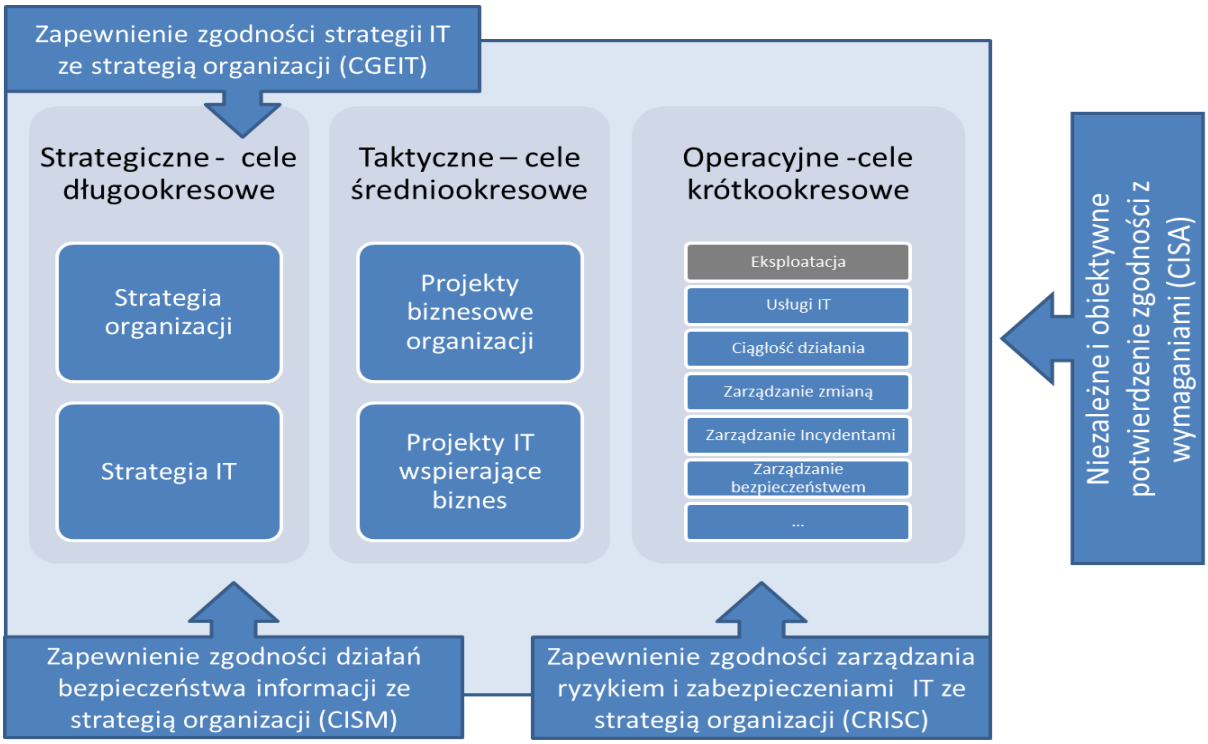
- Zapewnienia wysokiego poziomu bezpieczeństwa sektora publicznego, sektora prywatnego oraz obywateli w zakresie świadczenia lub korzystania z usług kluczowych oraz usług cyfrowych.
- Osiągnięcia zdolności do skoordynowanych w skali kraju działań służących zapobieganiu, wykrywaniu, zwalczaniu oraz minimalizacji skutków incydentów naruszających bezpieczeństwo systemów teleinformatycznych istotnych dla funkcjonowania państwa.
- Zwiększania potencjału narodowego oraz kompetencji w zakresie bezpieczeństwa w cyberprzestrzeni.

Zarządzanie ryzykiem jest mechanizmem zarządczym na poziomie planowania strategicznego, taktycznego i operacyjnego (przez ryzyko rozumie się wpływ niepewności na osiąganie tych rodzajów celów). Część ze zidentyfikowanych ryzyk będzie dotyczyła obszaru technologii stanowiąc wsad do zarządzania bezpieczeństwem informacji. Równocześnie na poziomie zarządzania bezpieczeństwem informacji musi zachodzić możliwość identyfikacji i szacowania ryzyka w celu doskonalenia systemu zarządzania bezpieczeństwem informacji, a przez to doboru właściwych zabezpieczeń organizacyjnych i technicznych. Do osiągnięcia powyższych celów jest niezbędne posiadanie właściwej wiedzy i pozyskanie lub wykształcenie kompetencji ludzi zdolnych do planowania i działania strategicznego, taktycznego oraz operacyjnego w zakresie:

1. Zarządzania ryzykiem
2. Zarządzania bezpieczeństwem informacji
3. Zarządzania ciągłością działania
4. Zarządzania usługami IT i wsparciem technicznym
5. Zarządzania projektami IT
6. Wytwarzania oprogramowania
7. Testowania oprogramowania
8. Audytowania obszaru cyberbezpieczeństwa
9. Testowania zabezpieczeń

Określenie zakresów kompetencji w obszarze cyberbezpieczeństwa wynika z zaleceń ISACA International. Na rysunku poniżej zaprezentowano obszary ICT związane z zachowanie bezpieczeństwa informatycznego w modelu ISACA.

Rysunek 2. Model bezpieczeństwa informatycznego ISACA



Źródło: Opracowanie własne na podstawie materiałów ISACA International

Na podstawie analizy modelu bezpieczeństwa informatycznego oraz obszarów wskazanych w dokumencie „Krajowe Ramy Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017-2022" dokonano określenia obszarów kompetencji niezbędnych do osiągnięcia celów Strategii. Wyniki przedstawiono w tabeli poniżej.

Tabela 1. Obszary kompetencji pracowników informatycznych niezbędne do osiągnięcia celów dokumentu Krajowe Ramy Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017-2022

Lp.	Obszar kompetencji	Obszar strategiczne
1.	Zarządzania ryzykiem	Zwiększenie bezpieczeństwa teleinformatycznego usług kluczowych i cyfrowych oraz infrastruktury krytycznej Wypracowanie i wdrożenie systemu zarządzania ryzykiem na poziomie krajowym Zbudowanie systemu ostrzegania użytkowników cyberprzestrzeni w zakresie ryzyka wynikającego z cyberzagrożeń Zbudowanie zdolności w zakresie analizy zagrożeń na poziomie krajowym Zwiększanie potencjału narodowego oraz kompetencji w zakresie bezpieczeństwa w cyberprzestrzeni
2.	Zarządzania bezpieczeństwem informacji	Zwiększenie bezpieczeństwa teleinformatycznego usług kluczowych i cyfrowych oraz infrastruktury krytycznej; Wypracowanie i wdrożenie systemu zarządzania ryzykiem na poziomie krajowym

Lp.	Obszar kompetencji	Obszar strategiczne
		Opracowanie i wdrożenie standardów oraz dobrych praktyk bezpieczeństwa sieci i systemów informatycznych Zbudowanie systemu ostrzegania użytkowników cyberprzestrzeni w zakresie ryzyka wynikającego z cyberzagrożeń Zbudowanie zdolności w zakresie analizy zagrożeń na poziomie krajowym Zbudowanie systemu bezpiecznej komunikacji na potrzeby bezpieczeństwa narodowego Audyty i testy bezpieczeństwa Zwiększanie potencjału narodowego oraz kompetencji w zakresie bezpieczeństwa w cyberprzestrzeni
3.	Zarządzania ciągłością działania	Zwiększenie bezpieczeństwa teleinformatycznego usług kluczowych i cyfrowych oraz infrastruktury krytycznej; Wypracowanie i wdrożenie systemu zarządzania ryzykiem na poziomie krajowym; Zbudowanie systemu ostrzegania użytkowników cyberprzestrzeni w zakresie ryzyka wynikającego z cyberzagrożeń Zwiększanie potencjału narodowego oraz kompetencji w zakresie bezpieczeństwa w cyberprzestrzeni
4.	Zarządzania usługami IT i wsparciem technicznym	Osiągnięcie zdolności do skoordynowanych w skali kraju działań służących zapobieganiu, wykrywaniu, zwalczaniu oraz minimalizacji skutków incydentów naruszających bezpieczeństwo systemów teleinformatycznych istotnych dla funkcjonowania państwa
5.	Zarządzania projektami	Rozbudowa zasobów przemysłowych i technologicznych na potrzeby cyberbezpieczeństwa Zbudowanie zdolności w zakresie analizy zagrożeń na poziomie krajowym Zbudowanie systemu ostrzegania użytkowników cyberprzestrzeni w zakresie ryzyka wynikającego z cyberzagrożeń
6.	Wytwarzania oprogramowania Testowanie oprogramowania	Rozbudowa zasobów przemysłowych i technologicznych na potrzeby cyberbezpieczeństwa Stymulowanie badań i rozwoju w obszarze bezpieczeństwa systemów teleinformatycznych
7.	Audytowanie obszaru cyberbezpieczeństwa	Zwiększanie zdolności do zwalczania cyberprzestępczości, w tym cyberszpiegostwa i zdarzeń o charakterze terrorystycznym, występującej w cyberprzestrzeni

Lp.	Obszar kompetencji	Obszar strategiczne
		Zbudowanie zdolności w zakresie analizy zagrożeń na poziomie krajowym Audyty i testy bezpieczeństwa
8.	Testowanie zabezpieczeń	Opracowanie i wdrożenie standardów oraz dobrych praktyk bezpieczeństwa sieci i systemów informatycznych Wypracowanie i wdrożenie systemu zarządzania ryzykiem na poziomie krajowym Zapewnienie bezpiecznego łańcucha dostaw Zbudowanie systemu ostrzegania użytkowników cyberprzestrzeni w zakresie ryzyka wynikającego z cyberzagrożeń Zwiększanie zdolności do zwalczania cyberprzestępczości, w tym cyberszpiegostwa i zdarzeń o charakterze terrorystycznym, występującej w cyberprzestrzeni Zbudowanie zdolności w zakresie analizy zagrożeń na poziomie krajowym Audyty i testy bezpieczeństwa Stworzenie warunków do bezpiecznego korzystania z cyberprzestrzeni przez obywateli

Źródło: Opracowanie własne

Powyższe obszary kompetencji mogą być reprezentowane przez różne specjalizacje, w ramach szeroko rozumianego zawodu „Informatyk", jednak pojęcie to jest bardzo pojemne i nieprecyzyjne, i zwyczajowo odnosi się głównie do obszaru „Zarządzania usługami IT i wsparcie techniczne". Dlatego też w niniejszym dokumencie proponujemy doprecyzowanie tego obszaru o dokładniejsze specjalizacje:

- Specjalista ds. zarządzania ryzykiem teleinformatycznym
- Specjalista ds. zarzadzania bezpieczeństwem informacji
- Specjalista ds. Ochrony Danych
- Specjalista ds. Ochrony Systemów IT
- Pentester – tester bezpieczeństwa systemów IT
- Specjalista ds. zarządzania ciągłością działania
- Specjalista ds. zarządzania projektami IT
- Specjalista ds. audytu usług IT
- Specjalista ds. audytu bezpieczeństwa IT
- Specjalista ds. help desk
- Administrator Sieci LAN/WAN
- Administrator IT
- Administrator Serwerów
- Administrator Systemów IT
- Administrator Baz Danych
- Administrator Aplikacji /oprogramowania wspierającego
- Inżynier Systemów IT

- Analityk Biznesowy IT
- Analityk Danych
- Programista
- Tester oprogramowania
- Architekt bezpieczeństwa IT
- Architekt Sieci IT
- Architekt Systemów IT[11]

Biorąc pod uwagę potrzeby i ważność poszczególnych specjalizacji i obszarów kompetencji metodą ekspercką określono wstępnie oczekiwaną dystrybucję poszczególnych specjalistów w ramach programu. Wyniki analizy przedstawiono w tabeli poniżej.

Tabela 2. Zestawienie proponowanej struktury zatrudnienia specjalistów w ramach programu Złota Setka

Lp.	Specjalizacja w kluczowych obszarach	Wstępna ocena stopnia wparcia
1.	Specjalista ds. zarządzania ryzykiem teleinformatycznym	20%
2.	Specjalista ds. zarzadzania bezpieczeństwem informacji	
3.	Specjalista ds. Ochrony Danych	
4.	Specjalista ds. Ochrony Systemów IT	
5.	Pentester – tester bezpieczeństwa systemów IT	
6.	Specjalista ds. zarządzania ciągłością działania	15%
7.	Specjalista ds. zarządzania projektami IT	
8.	Specjalista ds. audytu usług IT	
9.	Specjalista ds. audytu bezpieczeństwa IT	20%
10.		10%
11.	Specjalista ds. help desk	
12.	Administrator Sieci LAN/WAN	20%
13.	Administrator IT	
14.	Administrator Serwerów	
15.	Administrator Systemów IT	
16.	Administrator Baz Danych	
17.	Administrator Aplikacji /oprogramowania wspierającego	
18.	Inżynier Systemów IT	
19.	Analityk Biznesowy IT	15%
20.	Analityk Danych	
21.	Programista	
22.	Tester oprogramowania	
23.	Architekt bezpieczeństwa IT	
24.	Architekt Sieci IT	
25.	Architekt Systemów IT	

[11] Sieć informatyczna jako taka może być nośnikiem dla wielu systemów informacyjnych (w szczególności Informatycznych). Często wymaga oddzielnych, specyficznych dla tego poziomu kompetencji (reprezentowanych również przez różne certyfikaty), jak również nawet rozdzielności obowiązków w zarządzaniu tym obszarem względem innych obszarów IT.

Źródło: Opracowanie własne

Proponowana struktura zatrudnienia jest wynikiem pracy analitycznej wykonanej przez zespół ekspertów przygotowujących niniejsze opracowanie. Należy mieć na względzie, iż na etapie analizy brak jest dostępnych danych na temat rzeczywistej struktury zatrudnienia specjalistów IT w administracji, ich kompetencji i specjalizacji. Ze względu na przyszłą efektywność zarządzania programem rekomenduje się przygotowanie bazy danych specjalistów, którzy będą podlegać rekrutacji w ramach programu stypendialnego i jej stałą, regularną aktualizację w trakcie trwania programu.

Zaproponowana struktura ma na celu wskazanie wszystkich ról kluczowych dla utrzymania pełnego cyklu życia systemów teleinformatycznych i ich bezpieczeństwa. Poprzez cykl rozumiemy wszystkie działania związane z poprawnym (w tym bezpiecznym) zaprojektowaniem, wytworzeniem i utrzymaniem systemu informacyjnego i jego oprogramowania. Rozumiemy przez to także zbiór czynności umożliwiających wytworzenie nowego i wprowadzanie zmian do istniejącego systemu (oprogramowania, infrastruktury), reagowanie na incydenty i zapewnienie jego zakładanej jakości i ciągłości działania oraz możliwość potwierdzenia jego stanu faktycznego. Dlatego też bardzo wiele ról i kompetencji wchodzi w różne relacje ze sobą na różnych etapach życia systemu/oprogramowania. Jednocześnie biorąc pod uwagę zakres opracowania w dalszej części uwaga została skupiona bardziej na kompetencjach cyberbezpieczeństwa stąd biorąc pod uwagę kryteria naboru do programu wskazujemy kompetencje i certyfikaty związane bezpieczeństwem.

4. Typowanie kandydatów do programu

W programie mogą brać udział pracownicy administracji rządowej na poziomie centralnym (zatrudnienie w ministerstwach i urzędach wojewódzkich). Osoby do udziału w programie zgłaszane są w ramach procedury konkursowej (konkursu ogłaszanego przez Ministra właściwego ds. cyfryzacji) przez Kierowników danej jednostki.

Każdy z pracowników aby wziąć udział w programie musi spełnić, co najmniej następujące warunki:

- Posiadane kompetencje w zakresie co najmniej jednej ze wskazanych w regulaminie konkursu specjalizacji w zakresie bezpieczeństwa informatycznego.
- Zatrudnienie na stanowisku informatycznym i wykonywanie obowiązków związanych z jedną ze wskazanych specjalizacji.
- Potwierdzenie posiadanych kompetencji ważnym certyfikatem z proponowanej listy.

Listę proponowanych do uwzględnienia certyfikatów i ich umiejscowienie w ramach obszarów kompetencji prezentuje tabela poniżej.

Tabela 3. Propozycja certyfikatów jakimi powinni legitymować się kandydaci do programu „Złota Setka"

Lp.	Certyfikat	Opis certyfikatu	Obszary kompetencji	Organizacja certyfikująca
1.	ISO 31000 Risk Manager	ISO 31000 to rodzina standardów w zakresie zarządzania ryzykiem opracowanych przez Międzynarodową Organizację Normalizacyjną (ang. ISO – International Organization for Standardization). ISO 31000 definiuje zbiór zasad oraz ogólnych wytycznych dotyczących zarządzania ryzykiem. ISO 31000 dostarcza uniwersalny model zarządzania ryzykiem.	Zarządzanie ryzykiem	IRCA - International Register of Certificated Auditors -największa, międzynarodowa jednostka certyfikująca kursy dla audytorów. Szkolenia powinny być świadczone przez podmiot akredytowany przez IRCA lub inny podmiot o ustalonej rynkowej reputacji (np. CCJ VAT) czy też na innej drodze wyłoniony przez Ministerstwo
2.	ISO 27005 Risk Manager	Norma dedykowana dla zarządzania ryzykiem w bezpieczeństwie informacji. ISO 27005 ma zastosowanie do wszystkich typów organizacji (przedsiębiorstw, instytucji rządowych, organizacji non-profit), które zamierzają zarządzać ryzykami, które mogą spowodować naruszenie bezpieczeństwa informacji w tych organizacjach.	Zarządzanie ryzykiem	IRCA - International Register of Certificated Auditors -największa, międzynarodowa jednostka certyfikująca kursy dla audytorów. Szkolenia powinny być świadczone przez podmiot akredytowany przez IRCA lub inny podmiot o ustalonej rynkowej reputacji (np. CCJ VAT) czy też na innej drodze wyłoniony przez Ministerstwo
3.	ISO/IEC 27001 Audytor wewnętrzny / wiodący ISMS	ISO/IEC 27001 to norma międzynarodowa standaryzująca systemy zarządzania bezpieczeństwem informacji.	Zarządzanie bezpieczeństwem informacji	IRCA - International Register of Certificated Auditors -największa,

Lp.	Certyfikat	Opis certyfikatu	Obszary kompetencji	Organizacja certyfikująca
				międzynarodowa jednostka certyfikująca kursy dla audytorów. Szkolenia powinny być świadczone przez podmiot akredytowany przez IRCA lub inny podmiot o ustalonej rynkowej reputacji (np. CCJ VAT) czy też na innej drodze wyłoniony przez Ministerstwo
4.	ISO/IEC 22301 Audytor wewnętrzny / wiodący BCMS	ISO/IEC 22301 to norma międzynarodowa standaryzująca systemy zarządzania ciągłością działania.	Zarządzania ciągłością działania	IRCA - International Register of Certificated Auditors -największa, międzynarodowa jednostka certyfikująca kursy dla audytorów. Szkolenia powinny być świadczone przez podmiot akredytowany przez IRCA lub inny podmiot o ustalonej rynkowej reputacji (np. CCJ VAT) czy też na innej drodze wyłoniony przez Ministerstwo
5.	ITIL (Foundation/ Practicioner/Expert/Service Manager)	ITIL - to zbiór najlepszych praktyk w obszarze zarządzania usługami IT. Jest to biblioteka zawierające usystematyzowane podejście do zarządzania usługami IT, sprawdzone i polecane przez największe firmy informatyczne na świecie.	Zarządzania usługami IT i wsparciem technicznym	OGC (Office of Goverment Commerce) jest właścicielem znaku tow. ITIL. Szkolenia powinny odbywać się poprzez akredytowane jednostki szkoleniowe

Lp.	Certyfikat	Opis certyfikatu	Obszary kompetencji	Organizacja certyfikująca
6.	PMP, PRINCE 2, IPMA-B/C, Six sigma, SCRUM	Certyfikaty związane z zarządzaniem projektami:	Zarządzania projektami	
		PMP (Project Management Professional)- najbardziej rozpowszechniony z certyfikatów PMI (Project Management Institute). PMI jest właścicielem zbioru dobrych praktyk **PMBOK Guide** (Project Management Body of Knowledge Guide) jako zbioru dobrych praktyk.		Właścicielem PMP jest PMI PMI (Project Management Institute).
		PRINCE 2 – ceryfikat opracowany przez agende rządu brytyjskiego OGC (Office for Government Commerce) PRINCE2 oferuje trzy poziomy:		Proces certyfikacji w PRINCE2 jest nadzorowany przez firmę Axelos
		o Foundation,		
		o Practitioner; oraz		
		o Professional		
		Six Sigma została opracowana (przez firmę Motorola) jako metodyka zarządzania jakością. Celem Six Sigma jest usprawnianie procesów w firmie przez realizację projektów optymalizacyjnych. Elementy metodyki projektowej są inspirowane PMBOK Guide. Six Sigma oferuje kilka poziomów, najbardziej znane to:		
		o Green Belt		
		o Black Belt		

Lp.	Certyfikat	Opis certyfikatu	Obszary kompetencji	Organizacja certyfikująca
		Scrum - ramy postępowania zgodne ze „Scrum Guide" () Może mieć zastosowanie w realizacji projektów w oparciu o metodyki zwinne, zgodne z manifestem Agile (deklaracja wspólnych zasad dla zwinnych metodyk tworzenia oprogramowania) oferowany jest przez kilka organizacji, ale najpopularniejsza z nich to Scrum Alliance. Scrum Alliance oferuje 6 poziomów certyfikacji, z których najpopularniejsze są:		Scrum oferowany jest przez kilka organizacji, ale najpopularniejsza z nich to Scrum Alliance
		Certified Scrum Master (CSM),		
		Certified Scrum Professional (CSP)		
		Certified Scrum Trainer		
7.	CISSP	**Certified Information Systems Security Professional** - jest jednym z najbardziej rozpoznawanych certyfikatów w dziedzinie bezpieczeństwa informacji, który spełnia wymogi standardu ISO/IEC 17024:2003 (Ocena zgodności - Ogólne wymagania dotyczące jednostek certyfikujących osoby). O jego wartości świadczy także fakt, iż został on zatwierdzony przez amerykański Departament Obrony (DoD) CISSP przyznawany jest przez ISC2.	Zarządzanie bezpieczeństwem informacji Zarządzania ciągłością działania Zarządzania usługami IT i wsparciem technicznym Zarządzania projektami Testowanie / przełamywanie zabezpieczeń (ethical hacking)	ISC2 – organizacja skupiająca profesjonalistów w obszarze cyberbezpieczeństwa i bezpieczeństwa IT
8.	CIA	**Certified Internal Auditor** - powszechnie uznawane kwalifikacje z ogólnych wymagań audytu wewnętrznego.	Audytowanie obszarów biznesowych	The Institute of Internal Auditors

Lp.	Certyfikat	Opis certyfikatu	Obszary kompetencji	Organizacja certyfikująca
		Certyfikacja wymaga posiadania wiedzy i umiejętności w zakresie aktualnej praktyki audytu wewnętrznego, ale nie odnosi się do konkretnego obszaru (jak na przykład bezpieczeństwo informacji).		
9.	CISA	**Certified Information Systems Auditor** - certyfikat przyznawany przez ISACA (Information Systems Audit and Control Association stowarzyszenie o globalnej skali). Dedykowany audytorom bezpieczeństwa systemów informacyjnych	Audytowanie wszystkich obszarów przetwarzania informacji: strategii IT, wdrożeń IT, Ryzyka IT, eksploatacji IT, Bezpieczeństwa IT	ISACA International
		1. Zgodnie z rozporządzeniem Ministra Spraw Wewnętrznych i Administracji CISA znalazła się na liście certyfikatów uprawniających do prowadzenia kontroli projektów informatycznych i systemów teleinformatycznych.		
		2. Zgodnie z Ustawą z dnia 27 sierpnia 2009 r. o finansach publicznych, CISA jest certyfikatem uprawniającym do wykonywania zawodu audytora wewnętrznego w Polsce.		
10	CISM	**Certified Information Security Manager** dedykowany dla osób projektujących, oceniających i zarządzających systemami bezpieczeństwa w organizacjach. Certyfikat przyznawany przez ISACA.	Tworzenie i zarządzanie Systemem Bezpieczeństwa Informacji i Ciągłości Działania	ISACA International

Lp.	Certyfikat	Opis certyfikatu	Obszary kompetencji	Organizacja certyfikująca
11	CRISC	**Certified in Risk and Information Systems Control –** dedykowany dla profesjonalistów IT, którzy identyfikują ryzyka i zarządzają nimi poprzez opracowywanie, wdrażanie i utrzymywanie mechanizmów kontrolnych w systemach informacyjnych. Certyfikat przyznawany przez ISACA.	Zarządzanie ryzykiem i zabezpieczeniami IT	ISACA International
12	OSCP	**Offensive Security Certified Professional /Expert** – certyfikat dedykowany dla specjalistów testujących zabezpieczenia (tzw. etyczny hacking) Certyfikat przyznawany przez Offensive Security, najpopularniejszy z grona 5 oferowanych certyfikatów dotyczących testów penetracyjnych: • Offensive Security Certified Professional • Offensive Security Wireless Professional • Offensive Security Certified Expert • Offensive Security Exploitation Expert • Offensive Security Web Expert	Testowanie / przełamywanie zabezpieczeń (ethical hacking)	Offensive Security
13	CEH	**Certified Ethical Hacker** dedykowany dla specjalistów testujących zabezpieczenia (tzw. etyczny hacking) Certyfikat przyznawany przez EC-Council	Testowanie / przełamywanie zabezpieczeń (ethical hacking)	EC-Council

Lp.	Certyfikat	Opis certyfikatu	Obszary kompetencji	Organizacja certyfikująca
14	CompTIA Security +	Certyfikat przyznawany przez **Computing Technology Industry Association** (**CompTIA**) kierowany jest do specjalistów IT w zakresie podstawowych wymagań wobec bezpieczeństwa informacji.	Zarządzanie bezpieczeństwem informacji	CompTIA
15	GSEC GIAC	GIAC (Global Information Assurance Certification) – to program certyfikacyjny adresowany do specjalistów IT, oferuje około 40 specjalizowanych certyfikatów w obszarze ochrony przed cyberzagrożeniami, testów penetracyjnych, audytu, developmentu, i zarządzania incydentami.	Testowanie / przełamywanie zabezpieczeń (ethical hacking)	SANS Institute
		GSEC – koncentruje się na zapobieganiu atakom i detekcji, bezpiecznej komunikacji i koncepcjom architektury bezpieczeństwa sieci, jak również bezpieczeństwu systemów operacyjnych		Escal Institute of Advanced Technologies
16	CGEIT	**Certified in the Governance of Enterprise IT –**. Certyfikat adresowany do profesjonalistów odpowiedzialnych za strategiczne zarządzanie IT.Certyfikat przyznawany przez ISACA.	Zarządzanie ryzykiem i zabezpieczeniami IT	ISACA International
17	SSCP	**Systems Security Certified Practitioner –** certyfikat dla profesjonalistów IT związanych z tworzeniem zabezpieczeń	Zarządzanie bezpieczeństwem informacji	ISC2 – organizacja skupiająca profesjonalistów w obszarze

Lp.	Certyfikat	Opis certyfikatu	Obszary kompetencji	Organizacja certyfikująca
		dla informacji, bezpiecznym zarządzaniem środowiskiem sieciowym IT. Certyfikat przyznawany jest przez ISC2.		cyberbezpieczeństwa i bezpieczeństwa IT
18	CSIH	**Certified Computer Security Incident Handler** – certyfikat skierowany do specjalistów IT odpowiedzialnego za właściwe reagowanie na incydenty bezpieczeństwa i osiąganie aktualnej odporności na zagrożenia IT.	Obsługa incydentów bezpieczeństwa IT	Software Engineering Institute (SEI) – organizacja publiczno -prywatna; non-profit, prowadząca badania dla rządu USA

Źródło: Opracowanie własne

Powyższa lista nie wyczerpuje wszystkich możliwych certyfikatów związanych z cyberbezpieczeństwem, prezentuje natomiast najczęściej spotykane w Polsce certyfikaty określające kompetencje w prawidłowym i bezpiecznym modelu usług IT, ich eksploatacji i ewolucji, oraz możliwości potwierdzenia ich stanu.

Dynamiczna sytuacja w świecie technologii, zagrożeń i potrzeb biznesu powodują ciągły rozwój również tej dziedziny, jaką są szkolenia i certyfikacje. Dlatego należy oczekiwać, że prezentowany zbiór certyfikatów będzie ulegał zmianom w czasie, podobnie jak popularność poszczególnych certyfikatów. Stąd należy dokonywać oceny i doboru certyfikatów każdorazowo przy ogłaszaniu konkursu na stypendystów w ramach programu „Złota Setka".

Jednocześnie zwracamy uwagę, że w analizie celowo pominięto cały szereg certyfikatów „branżowych" (rozumianych jako dotyczących obsługi oprogramowania/ sprzętu danego producenta np. Oracle, Microsoft czy IBM). Zakres możliwości jest tu bardzo szeroki, a jednocześnie nie odnosi się on w sposób bezpośredni do tematyki programu „Złota Setka" czyli cyberbezpieczeństwa stąd uwzględnienie wybranych grup certyfikatów byłoby w naszej opinii naruszeniem zasady „neutralności technologicznej" stwarzając nieuzasadnione preferencje dla pracowników jednostek posiadających infrastrukturę w danej technologii w stosunku do innych oraz preferencje do producentów i właścicieli tych technologii.

W przyszłości możliwe będzie uwzględnienie tego typu certyfikatów jednak dopiero po przeprowadzeniu inwentaryzacji zasobów ludzkich i technicznych w zakresie bezpieczeństwa w jednostkach administracji rządowej objętych programem i wyłonieniu zestawu preferowanych technologii i dostawców (jeśli taka decyzja zostanie podjęta). Wtedy należy dokonać szerokiej analizy możliwych certyfikatów „branżowych" w kontekście bezpieczeństwa. Na obecnym etapie zakres ten wykracza poza objęty zleceniem i nie wnosi wartości do opracowania, a może być wręcz szkodliwy przy definiowaniu kryteriów w pierwszych konkursach prowokując uwagi o braku neutralności technologicznej i nieuzasadnionych preferencjach dla niektórych dostawców.

5. Analiza uwarunkowań prawnych związanych z programem stypendialnym

W rozdziale omówienie zostały prawne aspekty dotyczące możliwości wprowadzenia programów stypendialnych.

5.1. Wprowadzenie

Definicja określenia „stypendium"

Z punktu widzenia prawnego pojęcie „stypendium" nie zostało zdefiniowane. Bazując na doświadczeniu życiowym można przyjąć, że zwykle oznacza ono okresową pomoc finansową skierowaną przede wszystkim do uczniów, studentów, pracowników naukowych, artystów, sportowców lub innych grup społecznych bądź zawodowych. Zgodnie z definicją zawartą w słowniku języka polskiego, stypendium jest *„zapomogą pieniężną wypłacaną przez określony czas, zwykle z funduszów społecznych lub państwowych przeznaczoną dla uczącej się młodzieży, osób zajmujących się działalnością twórczą lub na prace specjalne*[12]".

Tak opisane stypendium zwykle stanowi świadczenie okresowe, to jest takie, które ma się powtarzać w regularnych odstępach czasu na podstawie i przez okres trwania danego stosunku prawnego.

[12] Mały Słownik Języka Polskiego pod red. E. Sabol, Wydawnictwo Naukowe PKW, Warszawa 2000

Poszczególne świadczenia okresowe zwykle są względem siebie samoistne i nie składają się na z góry określoną całość. Ta ostatnia cecha pozwala odróżnić świadczenia okresowe od poszczególnych rat świadczenia jednorazowego. W związku z tym nie będą zazwyczaj stanowiły „stypendium" świadczenia o z góry oznaczonej całkowitej wysokości, choćby ich wykonanie zostało rozłożone na raty.

Drugą istotną cechą świadczenia „stypendium" jest jego osobisty charakter rozumiany jako uprawnienie ściśle powiązane z osobą stypendysty i jego potrzebami. Dlatego też trudno byłoby uważać za stypendium świadczenia, do których prawo jest ukształtowane jako zbywalne i dziedziczone bez ograniczeń.

Do trzeciej istotnej cechy świadczenia stypendialnego trzeba zaliczyć jego celowy i ukierunkowany charakter. Stanowiąc w swoim założeniu pomoc w osiąganiu określonych celów (kształcenie, nauka, twórczość artystyczna lub realizacja innych określonych zadań) świadczenie to zachowuje swój sens tak długo, jak długo cele te mogą być osiągane[13]. Nie można zatem traktować jako stypendium świadczeń, choćby okresowych i osobistych, które mają być wypłacane uprawnionemu bez względu na to, czy oznaczone cele mogą i są przez niego realizowane (np. świadczenia alimentacyjne).

Z powyższego wynika, że z punktu widzenia prawa cywilnego stypendium należy określić jako świadczenie okresowe, osobiste i celowe, które ma wspierać uprawnionego w wypełnianiu oznaczonych zadań.

Generalne zasady przyznawania stypendium

Stypendia mogą być przyznawane w pierwszej kolejności na podstawie przepisów prawa, mających zwykle rangę ustawową (np. regulacje zawarte w ustawie o systemie oświaty lub ustawie o sporcie), których uszczegółowienie, w szczególności określenie zasad wypłacania, następuje w drodze regulacji pozaustawowych (np. rozporządzenia właściwego ministra). Istotne przy tym sposobie świadczenia pomocy stypendystom jest uprzednie zapewnienie odpowiedniego źródła finansowania zarówno w budżecie centralnym jak i budżetach poszczególnych jednostek zajmujących się wypłatą świadczeń. Ten sposób planowania i procedowania świadczeń stypendialnych jest charakterystyczny dla organów i instytucji publicznych.

Alternatywnie, stypendia są również przyznawane na podstawie rozstrzygnięcia podmiotu prowadzącego program stypendialny, będącego jednostką samorządu terytorialnego, uczelnią lub podmiotem prywatnym. W takiej sytuacji świadczenia te finansowane są z budżetów jednostek samorządu terytorialnego, dotacji lub funduszy własnych gromadzonych przez podmioty znajdujące poza strefą budżetową. W tej grupie stypendium nierzadko dochodzi do zawarcia pomiędzy beneficjentem a fundatorem umowy o stypendium, zwanej także umową stypendialną. Odnośna umowa może być ukształtowana jako dwustronnie lub jednostronnie zobowiązująca.

Przykładem pierwszego rodzaju jest chociażby umowa o tzw. stypendium fundowane, w której także i stypendysta zobowiązuje się do określonych świadczeń względem fundatora (np. do odbycia u niego praktyk, do uzgodnienia z nim tematu pracy dyplomowej, a także do pracy w jego zakładzie przez pewien czas po zakończeniu nauki).

Umowy drugiego rodzaju, przewidujące wypłacanie stypendium pod tytułem darmym, pojawiają się głównie w stosunkach z instytucjami powołanymi do wspierania określonych wartości lub interesów (stowarzyszenia, fundacje itp.) lub w stosunkach rodzinnych.

[13] Wyjaśnienie Ministra Finansów Departament Podatków Bezpośrednich, 1999.02.25, PB5/N-549/0226/99

Umowy o stypendium, tak jedno - jak i dwustronnie zobowiązujące mogą uzależnić prawo do pobierania świadczeń od osiągania przez beneficjenta – stypendystę określonych wyników w nauce lub w innej dziedzinie jego działalności.

5.2. Omówienie istniejących regulacji prawnych dotyczących stypendiów

Przed zarekomendowaniem i wybraniem rozwiązań wdrażających program stypendialny o roboczej nazwie „Złota Setka" celowym jest omówienie cech charakterystycznych poszczególnych stypendiów funkcjonujących w ustawodawstwie oraz obrocie prawnym Rzeczypospolitej Polskiej.

Stypendia dla uczniów

Najszerzej rozpoznawalną pomocą stypendialną są niewątpliwie świadczenia związane z nauką i edukacją. Rodzaje i cele świadczeń stypendialnych z tej grupy zostały przede wszystkim wskazane w ustawie z dnia 7 września 1991 roku o systemie oświaty. Pomoc tam uregulowana jest skierowana przede wszystkim do uczniów i ich rodzin.

Rozdział 8a ustawy o systemie oświaty wskazuje, iż ustawodawca wyróżnił dwa rodzaje pomocy. I tak, pomoc materialna może mieć charakter socjalny lub motywacyjny. Podział ten nawiązuje do celów postawionych przez ustawodawcę.

Warto zaznaczyć, że odnośnie pomocy materialnej o charakterze motywacyjnym, katalog fundatorów pozostaje otwarty. Dotyczy to stypendiów za wyniki w nauce oraz osiągnięcia sportowe. Nie ulega jednak wątpliwości, że podmioty prywatne mają także prawo do fundowania stypendiów socjalnych. Ustawa dopuszcza możliwość ubiegania się przez ucznia (i uzyskania) jednocześnie pomocy materialnej o charakterze socjalnym i motywacyjnym.

Ustawodawca bezpośrednio w samej ustawie uregulował podstawowe kryteria i zasady ubiegania się oraz przyznawania pomocy stypendialnej dla uczniów. Ustawa o systemie oświaty stanowi podstawę do przyznawania szeregu różnych świadczeń stypendialnych, w tym: (1) stypendium za wyniki w nauce lub sporcie, (2) stypendium Prezesa Rady Ministrów, (3) stypendium dla wybitnie uzdolnionych, (4) stypendium artystycznego oraz uprawnia wskazane w treści ustawy jednostki do opracowywania własnych programów pomocy mającej charakter stypendialny. W sprawie szczegółowych zasad przyznawania poszczególnych świadczeń ustawa o systemie oświaty odsyła do aktów prawnych niższego – rozporządzeń.

Należy zwrócić przy tym uwagę, że w art. 90n ust. 1 ustawy o systemie oświaty ustawodawca przesądził, że w sprawach świadczeń pomocy materialnej o charakterze socjalnym (w tym tzw. stypendium szkolnego) wydaje się decyzje administracyjne.

W przypadku innych stypendiów uregulowanych w tej ustawie, w szczególności świadczeń przyznawanych przez Prezesa Rady Ministrów, ustawodawca przewidział odmienną ścieżkę procedowania. Po pierwsze, kandydat do stypendium Prezesa Rady Ministrów powinien spełnić wymogi określone w art. 90h ustawy o systemie oświaty, z którego wynika m.in., że stypendium może być przyznane tylko jednemu z uczniów danej szkoły. Następnie w wydanym rozporządzeniu z dnia 14 czerwca 2005 roku w sprawie stypendiów Prezesa Rady Ministrów, ministra właściwego do spraw oświaty i wychowania oraz ministra właściwego do spraw kultury i ochrony dziedzictwa narodowego określona została szczegółowa wieloetapowa ścieżka administracyjna procedowania wniosków. Rozstrzygnięcie w tym wypadku nie wymaga przeprowadzenia konkursu opartego na złożonych kryteriach ocennych ani wydania decyzji administracyjnej, lecz świadczenia są przyznawane

maksymalnie jednemu wytypowanemu przez organy opiniodawcze reprezentantowi danej szkoły średniej spełniającego kryteria ustawowe.

Z przepisów ustawy o systemie oświaty wynika również, że jednostki samorządu terytorialnego mogą uruchamiać z własnej inicjatywy lokalne i regionalne programy stypendialne. Podstawę prawnych takich programów pomocy materialnej stanowi art. 90t ustawy o systemie oświaty. Zgodnie z tym przepisem jednostki samorządu terytorialnego, we współpracy z organizacjami pozarządowymi, mogą tworzyć regionalne lub lokalne programy: (1) wyrównywania szans edukacyjnych dzieci i młodzieży (wsparcie o charakterze socjalnym), (2) wspierania edukacji uzdolnionych dzieci i młodzieży (programy o charakterze motywacyjnym).

W takim wypadku, w ustawie o systemie oświaty (art. 90t ust. 4 tej ustawy) zapisano po prostu, że organ stanowiący jednostki samorządu terytorialnego w odpowiedniej uchwale określa szczegółowe warunki udzielania pomocy dzieciom i młodzieży, formy i zakres tej pomocy, w tym stypendia dla uzdolnionych uczniów oraz tryb postępowania w tych sprawach, uwzględniając w szczególności przedsięwzięcia sprzyjające eliminowaniu barier edukacyjnych, a także osoby lub grupy osób uprawnione do pomocy oraz potrzeby edukacyjne na danym obszarze. Ustawodawca pozostawił zatem fundatorom wyraźną swobodę w tworzeniu kryteriów i zasad przyznawania świadczeń.

Analizując uchwały wydawane przez jednostki samorządu terytorialnego w powyższych sprawach należy wskazać, że zawierają one autorski opis szczegółowych kryteriów, jakie powinien spełniać kandydat do otrzymania stypendium wraz z zasadami przyznawania punktacji, który stanowi podstawę do wskazania stypendystów. Powyższe jest również uzasadnione faktem, że liczba stypendiów jest zazwyczaj ściśle określona, a zatem rozstrzygniecie kwestii komu świadczenie zostanie przyznane musi nastąpić w drodze obiektywnego konkursu i stypendium otrzymuje z góry określona liczna osób, która uzyska największą liczbę punktów.

Stypendia sportowe

Bezpośredniej regulacji ustawowej doczekały się również zasady udzielania świadczeń stypendialnych za osiągniecia sportowe. W ustawie z dnia 25 czerwca 2010 roku o sporcie, ustawodawca przewidział, że stypendia sportowe mogą być ustanawiane i finansowe zarówno przez jednostki samorządu terytorialnego jak i organy centralne.

W myśl art. 31 ust. 3 tej ustawy organ stanowiący danej jednostki samorządu terytorialnego określa w drodze uchwały szczegółowe zasady, tryb przyznawania i pozbawiania oraz rodzaje i wysokość stypendiów sportowych, nagród i wyróżnień, biorąc pod uwagę znaczenie danego sportu dla tej jednostki samorządu terytorialnego oraz osiągnięty wynik sportowy. Tryb przyznawania tych świadczeń jest zazwyczaj podobny do modelu przyznawania przez jednostki samorządu terytorialnego stypendiów naukowych.

Istotne znaczenie w kontekście przyznawania stypendiów sportowych ma art. 32 tejże ustawy, w którym znalazły się dość szczegółowe regulacje upoważniające ministra właściwego do spraw kultury fizycznej do przyznawania stypendium sportowego członkom kadry narodowej.

Stosownie do treści art. 32 ust. 1 ustawy o sporcie, świadczenie stypendialne może być przyznawane za osiągnięte wyniki sportowe we współzawodnictwie międzynarodowym na okres do 24 miesięcy. Stypendium może otrzymać członek kadry narodowej, który zobowiąże się w formie pisemnej do realizacji programu przygotowań do igrzysk olimpijskich, igrzysk paraolimpijskich lub igrzysk głuchych albo programu przygotowań do mistrzostw świata lub mistrzostw Europy, opracowanego przez właściwy polski związek sportowy, oraz do udziału w tych zawodach.

Zgodnie z art. 32 ust. 1b przywołanej ustawy, podstawę ustalenia wysokości stypendium sportowego stanowi kwota 2300 zł, przy czym wysokość stypendium nie może przekroczyć 5,5-krotności tej kwoty.

Z art. 32 ust. 2 powyższej ustawy wynika również, że stypendia sportowe są finansowane ze środków budżetu państwa, z części, której dysponentem jest minister właściwy do spraw kultury fizycznej.

Co istotne, ustawodawca w ust. 5 wzmiankowanego przepisu wskazał, że przyznanie, wstrzymanie oraz pozbawienie stypendium sportowego następuje w drodze decyzji i już w samej ustawie wskazano podstawowe przesłanki do przyznania, wstrzymania oraz pozbawienia beneficjenta stypendium.

Finalnie, przepis art. 32 ust. 7 ustawy o sporcie odsyła do właściwego rozporządzenia, w którym minister właściwy do spraw kultury fizycznej określił: (1) szczegółowy tryb przyznawania członkowi kadry narodowej stypendium sportowego, a także wstrzymywania i pozbawiania tego stypendium, (2) przedział wysokości stypendium sportowego, stanowiący krotność kwoty bazowej, (3) czas, na jaki stypendium sportowe może zostać przyznane, (4) sposób i terminy wypłacania stypendium sportowego.

Interesującym rozwiązaniem jest, że w myśl art. 33 ustawy o sporcie, osoby pobierające stypendia sportowe są stypendystami sportowymi w rozumieniu przepisów ustawy z dnia 13 października 1998 r. o systemie ubezpieczeń społecznych a okres ich pobierania zalicza się do okresu zatrudnienia w rozumieniu przepisów ustawy z dnia 20 kwietnia 2004 r. o promocji zatrudnienia i instytucjach rynku pracy oraz do okresu zatrudnienia, od którego zależą uprawnienia pracownicze. Podstawę zaliczenia okresu pobierania stypendium sportowego stanowi zaświadczenie wydane przez podmiot wypłacający stypendium.

Stypendia dla twórców

Kolejnym rodzajem świadczeń stypendialnych uregulowanym ustawowo są stypendia artystyczne. Najczęstszą podstawą do przyznawania tego typu pomocy finansowej jest art. 7b ustawy z dnia 25 października 1991 roku o organizowaniu i prowadzeniu działalności kulturalnej oraz wydane na jego podstawie rozporządzenie ministra kultury i dziedzictwa narodowego z dnia 24 maja 2012 roku w sprawie szczegółowych warunków i trybu przyznawania stypendiów osobom zajmującym się twórczością artystyczną, upowszechnianiem kultury i opieką nad zabytkami oraz wysokości tych stypendiów.

Powyższe przepisy ustalają następujące zasady przyznawania stypendium:

- stypendium jest przyznawane w trybie konkursu ogłaszanego przez właściwego ministra;
- ogłoszenie o konkursie zawiera: (1) informację o przedmiocie konkursu, (2) terminie i miejscu składania wniosków, (3) warunkach udziału w konkursie, (4) procedurze i terminie rozstrzygnięcia konkursu;
- do ogłoszenia o konkursie załącza się: (1) regulamin konkursu, (2) wzory formularza wniosku zawierającego dane dotyczące wnioskodawcy oraz wykaz dokumentów, które należy dołączyć do wniosku, (3) wzór umowy stypendialnej;
- ogłoszenie o konkursie jest publikowane w Biuletynie Informacji Publicznej na stronie podmiotowej właściwego ministra.

Właściwy minister przyznaje stypendium wnioskodawcom wybranym w konkursie, określając jego wysokość i okres, na jaki zostaje przyznane. Informacja o przyznanych stypendiach jest również publikowana w Biuletynie Informacji Publicznej na stronie podmiotowej właściwego ministra.

Co istotne, z każdą z osób, którym przyznano stypendium zawiera się umowę stypendialną. Powyższa umowa stanowi podstawę wypłaty stypendium i określa m.in.: (1) wysokość stypendium oraz terminy wypłaty i sposób płatności, (2) obowiązki stypendysty i właściwego ministra, (3) tryb kontroli wykonania umowy, (4) termin i sposób rozliczenia stypendium.

Postępowanie w sprawie przyznawania stypendium artystycznego prowadzone jest każdorazowo na podstawie regulaminu, którego treść jest aktualizowana (poprawiana) przy kolejnych edycjach konkursu. Co istotne, właściwy minister zawiera ze stypendystą, według wzoru opracowanego odrębnie dla każdej edycji stypendium, umowę stypendialną, która reguluje wzajemne prawa i obowiązki stron.

Stypendia dla studentów

Polski ustawodawca uregulował również na poziomie ustawowym kwestię przyznawania stypendiów studentom. Nowa ustawa z dnia 29 lipca 2018 roku Prawo o szkolnictwie wyższym i nauce, póki co tylko częściowo weszła w życie. Wg stanu na dzień sporządzenia niniejszego opracowania, ustawa ta zakłada, iż stypendium może być przyznane studentowi przez jednostkę samorządu terytorialnego lub osobę fizyczną bądź prawną.

W dniu 1 października 2019 roku wejdą w życie m.in. przepisy art. 86-94 Prawa o szkolnictwie wyższym i nauce, zawierające szczegółowe regulacje dotyczące stypendiów przyznawanych w drodze decyzji administracyjnej, w tym stypendium socjalnego, stypendium dla osób niepełnosprawnych i stypendium rektora.

Dodatkowo, omawiana ustawa przyznaje ministrowi właściwemu do spraw szkolnictwa wyższego prawo do przyznawania stypendiów dla zdolnych studentów i młodych naukowców. Ponadto, zgodnie z art. 364 prawa o szkolnictwie wyższym i nauce, Prezes Rady Ministrów jest również uprawniony do przyznawania nagród za osiągnięcia naukowe.

Aktualnie trwają prace nad stworzeniem (i uchwalaniem) odpowiednich przepisów wykonawczych konkretyzujących zasady przyznawania i wypłacania świadczeń stypendialnych.

Stypendia prywatne oraz międzynarodowe

Pozostałe formy stypendialne funkcjonujące w obrocie prawnym związane są ze środkami przyznawanymi przez osoby fizyczne lub prawne funkcjonujące poza sferą budżetowa. Można wyróżnić sporą grupę pomocy materialnej udzielanej przez polskiej jak i zagraniczne organizacje pozarządowe. Podmioty te mogą z własnej inicjatywy przyznawać i wypłacać stypendia oraz prowadzić programu stypendialne.

Przyznawanie stypendium prywatnego wiąże się zwykle z zawarciem przez strony umowy stypendialnej. Jak już wspomniano na wstępie tej części opracowania, pojęcie „stypendium” czy „umowa stypendialna” nie zostały wprost zdefiniowane w przepisach prawa. Umowa stypendialna stanowi zatem umowę nienazwaną, która może być zawierana na zasadzie tzw. swobody umów wynikającej z art. 353^1 Kodeksu cywilnego.

W praktyce umowa stypendialna zwykle określa wysokość stypendium, terminy i zasady jego wypłaty, a także warunki i obowiązki jakie musi wypełnić stypendysta, aby móc otrzymać i zachować przyznane mu środki.

Od wielu lat w polskich realiach funkcjonują różne międzynarodowe lub stricte zagraniczne instytucje oferujące możliwość otrzymania stypendium, związanego zwykle z czasowym wyjazdem lub wymianą międzynarodową.

Jakkolwiek w polskich realiach prawnych na próżno jest szukać programów zbliżonych do założeń koncepcji stypendium „Złota Setka" przeznaczonych dla osób zatrudnionych w administracji publicznej, to zdarzają się oferty stypendium spoza sfery budżetowej skierowanej do urzędników państwowych. Przykładem takiego projektu jest program stypendialny „Young Leaders' Program" powstały z inicjatywy japońskiego Ministerstwa Edukacji, Kultury, Sporu, Nauki i Technologii, który jest skierowany, przy współpracy z Kancelarią Prezesa Rady Ministrów, wprost do pracowników administracji publicznej.

Regulacje podatkowe związane ze stypendiami

Co do zasady, wszelkiego rodzaju dochody osiągane przez obywateli podlegają opodatkowaniu podatkiem dochodowym od osób fizycznych, chyba że są one objęte innym podatkiem, na przykład podatkiem od spadków i darowizn.

Art. 20 ust. 1 ustawy o podatku dochodowym od osób fizycznych wskazuje, że za przychody podatkowe z tak zwanych innych źródeł uważa się między innymi stypendia. W praktyce część świadczeń stypendialnych wypłacanych przez jednostki samorządu terytorialnego i organizacje pozarządowe jest kwalifikowanych jako przychody podlegające podatkowi dochodowemu. Zdarza się również, że stypendia mogą zostać uznane za darowiznę podlegającą podatkowi od spadków i darowizn[14].

Wyjątki od zasady powszechności opodatkowania podatkiem dochodowym zostały określone w art. 21 ustawy, zawierającym tzw. wyłączenia przedmiotowe. Zgodnie z tym przepisem niektóre rodzaje dochodów o charakterze stypendialnym są w całości lub części wolne od podatku dochodowego.

I tak, w myśl art. 21 ust. 1 pkt 39 i następnych ustawy o podatku dochodowym od osób fizycznych, wolne od podatku dochodowego są:

- stypendia i zapomogi, o których mowa w ustawie z dnia 20 lipca 2018 roku Prawo o szkolnictwie wyższym i nauce, oraz stypendia otrzymywane w ramach programów lub przedsięwzięć, o których mowa w art. 376 ust. 1 tej ustawy; w przypadku stypendiów przyznawanych przez osobę fizyczną lub osobę prawną niebędącą państwową ani samorządową osobą prawną zwolnienie ma zastosowanie, o ile zasady ich przyznawania zostały zatwierdzone przez ministra właściwego do spraw szkolnictwa wyższego i nauki,
- stypendia i inne środki finansowe, o których mowa w art. 18 ust. 2 pkt 1 ustawy z dnia 7 lipca 2017 r. o Narodowej Agencji Wymiany Akademickiej,
- stypendia przyznawane przez instytuty naukowe Polskiej Akademii Nauk oraz instytuty badawcze, z ich funduszy stypendialnych,
- stypendia, o których mowa w art. 70b ustawy z dnia 30 kwietnia 2010 r. o Polskiej Akademii Nauk (przepis wchodzi w życie z dniem 1 stycznia 2019 roku),
- stypendia i inne świadczenia otrzymywane w ramach programu wymiany stypendialnej Polsko-Amerykańskiej Komisji Fulbrighta,
- świadczenia pomocy materialnej dla uczniów i osób uczestniczących w innych formach kształcenia, pochodzące z budżetu państwa, budżetów jednostek samorządu terytorialnego oraz ze środków własnych szkół przyznane na podstawie przepisów o systemie oświaty oraz inne stypendia

[14] interpretacja podatkowa Urzędu Skarbowego w Krośnie 2007.03.15, US.PDF/415-10/07

za wyniki w nauce, których zasady przyznawania zostały zatwierdzone przez ministra właściwego do spraw oświaty i wychowania,

- stypendia dla uczniów i studentów, których wysokość i zasady udzielania zostały określone w uchwale organu stanowiącego jednostki samorządu terytorialnego, oraz stypendia dla uczniów i studentów przyznane przez organizacje, o których mowa w art. 3 ust. 2 i 3 ustawy o działalności pożytku publicznego, na podstawie regulaminów zatwierdzonych przez organy statutowe udostępnianych do publicznej wiadomości za pomocą Internetu, środków masowego przekazu lub wykładanych (wywieszanych) dla zainteresowanych w pomieszczeniach ogólnie dostępnych – do wysokości nieprzekraczającej w roku podatkowym kwoty 3800 zł.

Powyższy katalog zwolnień jest zamknięty, co oznacza, że ewentualne inne świadczenia stypendialne niewymienione w art. 21 ust. 1 ustawy o podatku dochodowym od osób fizycznych, w tym np. wypłacane w ramach programu „Złota Setka", podlegają temu podatkowi w myśl art. 20 ust. 1 tej ustawy.

Podsumowanie

Programy stypendialne funkcjonujące w polskim obrocie prawnym oferują pomoc finansową różnym grupom zawodowym i społecznym, najczęściej jednak są one związane z działalnością szkolno-naukową, sportową lub ewentualnie artystyczną.

W przypadku stypendiów finansowanych ze środków publicznych, w szczególności pozostających w gestii organów centralnych, w tym Prezesa Rady Ministrów lub ministrów, podstawą do ich przyznawania są przepisy ustawowe, które znajdują ewentualne uszczegółowienie w innych aktach prawnych niższego rzędu, to jest rozporządzeniach.

W programach stypendialnych organizowanych przez organy administracji publicznej można zaobserwować trzy podstawowe zasady procedowania wniosków i przyznawania stypendiów:

1) „metoda decyzji administracyjnej" – polegającą na procedowaniu wniosków o przyznanie stypendium w ramach postępowania administracyjnego, w ramach którego uprawniony organ weryfikuje, czy wnioskodawca spełnia określone w przepisach powszechnie obowiązującego prawa wymogi i które to postępowanie kończy się wydaniem stosownego rozstrzygnięcia – decyzji administracyjnej. Postępowanie to jest charakterystyczne przede wszystkim dla stypendiów mających charakter zapomogi socjalnej (niektóre stypendia dla uczniów i studentów) oraz stypendiów sportowych;
2) „metoda ścieżki formalno-administracyjnej" – polegającą na składaniu wniosku o przyznanie stypendium nie bezpośrednio do podmiotu, w którego gestii pozostają środki, ale wnioskowania za pośrednictwem wskazanych w przepisach prawa powszechnie obowiązującego komórek organizacyjnych, instytucji i organów, które mają za zadanie opiniowanie i zweryfikowanie wniosków, będąc często uprawnionymi do wybrania tych wniosków, które będą procedowane dalej, celem wskazania organowi przyznającego stypendium odpowiednich kandydatów, którzy staną beneficjentami stypendiów. Model ten jest w szczególności stosowany w przypadku stypendium dla uczniów szkół średnich przyznawanego przez Prezesa Rady Ministrów;
3) „metoda konkursowa" – polegająca na przygotowywaniu przez organ wskazany w przepisach prawa powszechnie obowiązującego odpowiednich regulaminów i kryteriów konkursowych pozwalających na wyłonienie przez ten organ „najlepszych", to uzyskujących najwyższą punktację (ocenę) wnioskodawców, którym zostaje przyznane stypendium. Model ten często zakłada konieczność zawarcia pomiędzy stypendystą a fundatorem stosownej umowy, w której ten

pierwszy zobowiązuje się do wykonywania lub zaniechania konkretnych czynności. W odróżnieniu od metod szczegółowo uregulowanych w przepisach prawa powszechnie obowiązującego ten sposób procedowania daje większą elastyczność fundatorowi, pozwalając mu na ustalanie zasad konkursu, tak aby pasowały one do aktualnych potrzeb i celów, jakie mają być realizowane przez stypendystów oraz dokonywanie ich ewentualnej adaptacji w kolejnych edycjach programu stypendialnego. Powyższy sposób procedowania wydaje się być ponadto dedykowany do programów stypendialnych, w których została ściśle określona maksymalna liczba beneficjentów stypendiów będąca znacząco mniejsza od liczby potencjalnych kandydatów. W ramach sfery budżetowej model ten jest w szczególności stosowany w przypadku stypendium dla twórców przyznawanego przez ministra właściwego dla spraw kultury i ochrony dziedzictwa narodowego. Ponadto, jest on również dość często stosowany przy wyborze stypendystów z programów realizowanych przez jednostki samorządu terytorialnego oraz sektor prywatny.

5.3. Analiza zasad wynagradzania pracowników administracji publicznej

Zagadnienia ogólne

Zasady wynagradzania pracowników zatrudnionych w administracji publicznej zostały uregulowane w szeregu aktów prawnych i są one uwarunkowane między innymi tym czy dany pracownik pozostaje jednocześnie członkiem korpusu służby cywilnej czy też takiego statusu nie posiada. Zasady wynagradzania członków korpusu służby cywilnej reguluje między innymi ustawa z dnia 21 listopada 2008 roku o służbie cywilnej, jak również wydane na jej podstawie akty wykonawcze, w tym w szczególności rozporządzenie Prezesa Rady Ministrów z dnia 29 stycznia 2016 roku w sprawie określenia stanowisk urzędniczych, wymaganych kwalifikacji zawodowych, stopni służbowych urzędników służby cywilnej, mnożników do ustalania wynagrodzenia oraz szczegółowych zasad ustalania i wypłacania innych świadczeń przysługujących członkom korpusu służby cywilnej.

Reguły wynagradzania pracowników administracji publicznej niebędących natomiast członkami korpusu służby cywilnej określa przede wszystkim ustawa z dnia 16 września 1982 roku o pracownikach urzędów państwowych oraz wydane na jej podstawie rozporządzenie Rady Ministrów z dnia 2 lutego 2010 roku w sprawie zasad wynagradzania pracowników niebędących członkami korpusu służby cywilnej zatrudnionych w urzędach administracji rządowej i pracowników innych jednostek.

Niezależnie od tego każda z jednostek czy urzędów, w momencie zatrudnienia pracowników, staje się ich pracodawcą, wobec czego, bez względu na to jaką podstawę prawną przyjęto dla zatrudnienia danego pracownika i jakie przepisy regulują jego status, na pracodawcy ciążą określone obowiązki wynikające ze stosunku pracy, przy czym większość tych obowiązków regulują przepisy Kodeksu pracy, które mają w tym zakresie bezpośrednie zastosowanie.

Pomimo zatem, iż pracownicy sfery budżetowej podlegają odrębnym przepisom regulującym zasady ich zatrudnienia, to jednak w sprawach wprost w nich nieuregulowanych zastosowanie mają przepisy ogólne prawa pracy. Tak jest na przykład w przypadku ustalania wynagrodzenia za urlop wypoczynkowy oraz ekwiwalentu pieniężnego za urlop niewykorzystany w naturze.

Zasady wynagradzania członków korpusu służby cywilnej

W przypadku członków korpusu służby cywilnej, na ich wynagrodzenie składają się zarówno elementy stałe, to jest wynagrodzenie zasadnicze, dodatek za wieloletnią pracę w służbie cywilnej, dodatek służby cywilnej oraz dodatek funkcyjny, jak również składniki dodatkowe tego wynagrodzenia, takie jak dodatek zadaniowy, nagroda jubileuszowa, nagroda za szczególne osiągniecia oraz dodatkowe

wynagrodzenie roczne. Członkowi korpusu służby cywilnej przysługuje także jednorazowa odprawa w związku z przejściem na rentę z tytułu niezdolności do pracy lub w związku z przejściem na emeryturę.

Analizując pokrótce poszczególne składniki stałe wynagrodzenia członka korpusu służby cywilnej należy zauważyć, że: a) wynagrodzenie zasadnicze przewidziane dla zajmowanego stanowiska pracy ustala dyrektor generalny jednostki z zastosowaniem mnożników kwoty bazowej, której wysokość ustaloną według odrębnych zasad określa ustawa budżetowa; b) dodatek za wieloletnią pracę jest naliczany jako odsetek wynagrodzenia zasadniczego, co oznacza, że każda podwyżka wynagrodzenia zasadniczego powoduje automatyczną podwyżkę ustalonej kwoty dodatku; c) dodatek służby cywilnej przysługuje członkowi korpusu służby cywilnej, który stał się urzędnikiem, przy czym wysokość tego dodatku, podobnie jak wynagrodzenia zasadniczego, jest naliczana za pomocą mnożnika kwoty bazowej; d) dodatek funkcyjny dotyczy członków korpusu służby cywilnej zatrudnionych na stanowiskach wyższych i wraz z wynagrodzeniem oraz dodatkiem za wieloletnią pracę stanowi wynagrodzenie tej kategorii zatrudnionych w służbie cywilnej, a jego wysokość jest ustalana za pomocą mnożnika kwoty bazowej.

Niezależnie od elementów stałych wynagrodzenia, członek korpusu służby cywilnej może otrzymywać określone ustawą dodatkowe świadczenia pieniężne. Pierwszym składnikiem wynagrodzenia członka korpusu służby cywilnej, który nie ma charakteru stałego, jest dodatek zadaniowy, który może zostać przyznany za wykonywanie dodatkowych, powierzonych przez pracodawcę zadań na okres wykonywania tych zadań, ze środków przeznaczonych na wynagrodzenia. Wysokość, okres przyznawania oraz charakter zadań, za jakie zostaje przyznany dodatek, stanowią przedmiot arbitralnej decyzji dyrektora generalnego jednostki. Innym składnikiem dodatkowym wynagrodzenia członka korpusu służby cywilnej jest tzw. nagroda jubileuszowa, której zasady otrzymywania przez członków korpusu służby cywilnej, w przeciwieństwie do dodatku zadaniowego, zostały jasno określone w ustawie. Nagroda jubileuszowa jest świadczeniem pieniężnym o charakterze cyklicznym, która jest przyznawana po przepracowaniu określonej liczby lat, a uzyskanie tego świadczenia przez członka korpusu służby cywilnej jest obligatoryjne, ma charakter roszczeniowy i nie jest zależne od wyników pracy.

Ustawa o służbie cywilnej upoważnia także dyrektora generalnego jednostki do przyznawania członkom korpusu służby cywilnej nagród za szczególne osiągnięcia w pracy zawodowej. Jeśli chodzi o kryteria przyznawania i wysokość tych nagród, to sytuacja w tym zakresie jest zbieżna z dodatkami zadaniowymi i polega na dużej uznaniowości, chociażby z tego powodu, że nie zdefiniowano pojęcia „szczególne osiągnięcia w pracy zawodowej".

Kolejnym elementem wynagrodzenia członka korpusu służby cywilnej jest dodatkowe wynagrodzenie roczne, którego podstawę prawną stanowi ustawa z dnia 12 grudnia 1997 roku o dodatkowym wynagrodzeniu rocznym dla pracowników jednostek sfery budżetowej**.** Dodatkowe wynagrodzenie roczne ustala się w wysokości określonej procentowo sumy wynagrodzenia za pracę otrzymanego przez pracownika w ciągu roku kalendarzowego, przy czym do sumy wynagrodzenia wlicza się otrzymane w ciągu roku wynagrodzenie i inne świadczenia ze stosunku pracy przyjmowane do obliczenia ekwiwalentu pieniężnego za urlop wypoczynkowy, wynagrodzenie za urlop wypoczynkowy, a także wynagrodzenie za czas pozostawania bez pracy przysługujące pracownikowi, który podjął pracę w wyniku przywrócenia do pracy.

Zasady wynagradzania pracowników niebędących członkami korpusu służby cywilnej

Podobne zasady wynagradzania obowiązują pracowników urzędów państwowych niebędących członkami korpusu służby cywilnej. Na ich uposażenie składa się przede wszystkim wynagrodzenie zasadnicze, które jest zależne od zajmowanego stanowiska, posiadanych kwalifikacji zawodowych, jakości oraz stażu pracy. Ponadto pracownikom urzędów państwowych przysługuje dodatek za wieloletnią pracę w urzędach państwowych, a także nagroda jubileuszowa, która jest przyznawana po przepracowaniu określonej liczby lat. Z tytułu okresowego zwiększenia obowiązków służbowych lub powierzenia dodatkowych zadań albo ze względu na charakter pracy lub warunki wykonywania pracy kierownik urzędu lub jednostki może natomiast przyznać pracownikowi dodatek specjalny na czas określony, a w indywidualnych przypadkach także na czas nieokreślony.

Analogicznie jak w przypadku członków korpusu służby cywilnej, także pracownikom urzędów państwowych nieposiadającym takiego statusu przysługuje dodatkowe wynagrodzenie roczne na podstawie ustawy z dnia 12 grudnia 1997 roku o dodatkowym wynagrodzeniu rocznym dla pracowników jednostek sfery budżetowej. Dodatkowo w urzędach państwowych tworzy się zakładowy fundusz nagród z przeznaczeniem na nagrody za szczególne osiągnięcia w pracy zawodowej. Wreszcie pracownikom urzędów państwowych przechodzącym na emeryturę lub rentę z tytułu niezdolności do pracy przysługuje jednorazowa odprawa.

Możliwości wdrożenia dodatkowego programu motywacyjnego

Interpretacja obowiązujących przepisów prawa pozwala stwierdzić, że ustawodawca dosyć kategorycznie określił zasady ustalania wynagrodzenia pracowników administracji publicznej. Dokładnie określono poszczególne składniki wynagrodzenia, a także zasady ich przyznawania. Wynagrodzenie uzależnione jest przede wszystkim od zaszeregowania danego pracownika, pełnionej przez niego funkcji oraz stażu pracy. Ustawodawca zdecydował się także dodatkowo premiować pracowników ze względu na okresowe zwiększenia ich obowiązków służbowych lub powierzenia dodatkowych zadań oraz z uwagi na charakter pracy lub warunki jej wykonywania. Istotne jest przy tym, że katalog składników wynagrodzenia pracowników administracji publicznej, zarówno członków korpusu służby cywilnej jak i pozostałych pracowników, wydaje się być zamknięty, zagadnienie to zostało uregulowane przez ustawodawcę w sposób wyczerpujący.

Oczywiście w kwestiach zatrudnienia, które nie zostały uregulowane odrębnymi przepisami, do pracowników administracji publicznej stosuje się ogólne zasady prawa pracy, niemniej jednak należy uznać, że zasady wynagradzania pracowników administracji publicznej zostały uregulowane w przepisach odrębnych w sposób kompleksowy, wyczerpujący, w konsekwencji czego posiłkowanie się w tym zakresie ogólnymi przepisami prawa pracy jest nieuzasadnione.

Przeprowadzona powyżej analiza prowadzi do wniosku, że na gruncie obowiązujących **obecnie przepisów prawa wydaje się nie być możliwym wdrożenie motywacyjnego programu stypendialnego dla specjalistów z obszaru cyberbezpieczeństwa pracujących w administracji publicznej, w ramach któregokolwiek ze składników przysługującego im wynagrodzenia**. Zarówno bowiem w przepisach odnoszących się do pracowników będących członkami korpusu służby cywilnej, jak również w przepisach regulujących zasady wynagradzania pracowników urzędów państwowych spoza grona korpusu służby cywilnej, ustawodawca wyraźnie określił zasady wynagradzania, zdefiniował enumeratywnie składniki wynagrodzenia, jak również wskazał kryteria przyznawania poszczególnych składników tego wynagrodzenia.

Ze względu na swoją specyfikę, w tym w szczególności zaadresowanie programu stypendialnego do bardzo konkretnej grupy pracowników administracji publicznej, w tym także ze względu na objęcie

tym programem zarówno członków korpusu służby cywilnej jak też pracowników, **którzy nie posiadają takiego statusu, wydaje się, że program stypendialny nie może zostać przyporządkowany do żadnego z istniejących obecnie składników wynagrodzenia pracowników administracji publicznej**. W szczególności należy wykluczyć uznanie stypendium za element wynagrodzenia zasadniczego, nie sposób uznać także, aby mogło ono stanowić dodatek funkcyjny, gdyż według założeń tego programu, stypendium może zostać przyznane specjalistom spełniającym najwyższe kryteria wiedzy fachowej, niemniej jednak elementem determinującym w tym zakresie nie jest ani funkcja pełniona w administracji publicznej ani zajmowane stanowisko. Stypendium nie może również zostać zakwalifikowane jak dodatek stażowy, albowiem staż pracy może być ewentualnie jednym z kryteriów do objęcia danego pracownika programem stypendialnym. Brak jest wreszcie podstaw, aby stypendium było przyznawane w formie nagrody przez kierownika jednostki. Nagroda bowiem z założenia ma charakter wypadkowy, jest przyznawana za szczególne osiągnięcia zawodowe, a ponadto, co istotne, jest przyznawana dopiero *post factum*. Nie sposób wreszcie potraktować stypendium jako dodatku z tytułu okresowego zwiększenia obowiązków służbowych lub powierzenia pracownikowi dodatkowych zadań, a to dlatego, że założeniem programu stypendialnego jest motywowanie pracowników wyselekcjonowanych ze względu na wyróżniający ich stopień fachowości do pozostania w strukturach administracji publicznej, bez jednoczesnego zwiększania zakresu ich obowiązków.

Podsumowując zatem powyższe rozważania należy stwierdzić, mając na uwadze założenia programu stypendialnego, że chociaż obowiązujące przepisy prawa nie zawierają regulacji pozwalających na wypłacanie dodatkowego świadczenia stypendialnego w ramach któregokolwiek z ustawowo określonych składników wynagrodzenia, to **jednak brak jest ogólnych przeciwskazań do objęcia tych pracowników specjalnym programem motywacyjnym**, zwłaszcza, że ma się to przyczynić do zahamowania odpływu tych pracowników ze struktur administracji publicznej, a tym samym doprowadzić do zwiększenia bezpieczeństwa państwa. Wdrożenie programu motywacyjnego jest zatem nie tylko uzasadnione interesem państwowym, ale także wydaje się być skutecznym narzędziem zatrzymania specjalistów z tej branży w administracji publicznej.

Przeszkody dla wdrożenia programu stypendialnego nie stanowią również przepisy aktów prawnych regulujących kwestie związane z finansami publicznymi. W szczególności przeciwwskazań w tym zakresie nie sposób znaleźć w ustawie z dnia 27 sierpnia 2009 roku o finansach publicznych. W przedmiotowej ustawie określono bowiem wprost, że wydatki budżetu państwa są przeznaczone między innymi na funkcjonowanie organów władzy publicznej, zadania wykonywane przez administrację rządową czy chociażby dotacje na zadania określone odrębnymi ustawami. Chodzi tu o wydatki na wypełnianie funkcji władczych, związanych ze stosowaniem przymusowym prawa oraz zapewnieniem obronności i bezpieczeństwa, czyli wydatki, od których zależy istnienie państwa oraz wypełnianie przez państwo podstawowych funkcji politycznych, chroniących zarazem wolności obywatelskie. Niewątpliwie zatem program stypendialny skierowany do specjalistów z zakresu cyberbezpieczeństwa mieści się w sferze wydatków przeznaczonych na funkcjonowanie organów władzy związanych z obronnością i bezpieczeństwem państwa.

W związku z objęciem danego pracownika programem stypendium motywacyjnego uzasadnione może okazać się powiadomienie o tym fakcie dyrektora generalnego urzędu - w przypadku członków korpusu służby cywilnej, albo kierownika urzędu - w odniesieniu do pracowników niebędących członkami korpusu służby cywilnej. Zarówno bowiem w stosunku pracowników – członków korpusu służby cywilnej, jak i pracowników nieposiadających tego statusu, przepisy prawa wymagają uzyskania przez

pracownika zgody na podjęcie dodatkowej działalności zarobkowej. W przypadku członków korpusu służby cywilnej ustawodawca przewidział obowiązek uzyskania pisemnej zgody na podjęcie dodatkowego zatrudnienia, a zatem wyłącznie takiego na podstawie umowy o pracę, natomiast w odniesieniu do urzędników służby cywilnej, w tym także osób zajmujących wyższe stanowiska w służbie cywilnej, zgody wymaga już każda działalność zarobkowa, w tym także ta podejmowana na podstawie umów cywilnoprawnych czy w ramach prowadzonej działalności gospodarczej (vide: art. 80 ustawy o służbie cywilnej). W przypadku zaś pracowników niebędących członkami korpusu służby cywilnej, ustawa stanowi, iż nie mogą oni podejmować dodatkowego zatrudnienia bez uzyskania uprzedniej zgody kierownika urzędu, w którym są zatrudnieni (vide: art. 19 ustawy o pracownikach urzędów państwowych).

W zależności zatem od ostatecznego kształtu programu stypendialnego, udział w nim danego pracownika może natomiast wymagać uzyskania na to zgody ze strony właściwego kierownika jednostki zatrudniającej stypendystę.

5.4. Rekomendacje prawne

W kontekście omawianej koncepcji stypendium „Złota Setka" wydaje się, że najodpowiedniejszym modelem zorganizowania postępowania związanego z procedowaniem i przyznawaniem zakładanych świadczeń motywacyjnych byłaby tzw. metoda konkursowa. Wymaga ona co prawda i tak umocowania na poziomie przepisów prawa powszechnie obowiązującego (niezbędnym jest przynajmniej określone źródła finansowania i podstawy prawnej do zorganizowania programu), ale pozwala na stworzenia elastycznego kryterium wyboru stypendystów i dostosowania zobowiązań nakładanych na beneficjentów programu do oczekiwań oraz potrzeb fundatora.

Celowym wydaje być zatem wprowadzenie do obrotu prawnego regulacji wzorowanych na zasadach, na jakich przyznawane są stypendia opisane w art. 7b ustawy z dnia 25 października 1991 roku o organizowaniu i prowadzeniu działalności kulturalnej.

W przypadku programu typu „Złota Setka", należałoby rozważyć zapisanie na poziomie odpowiedniej ustawy, między innymi, iż:

- minister właściwy do spraw cyfryzacji może przyznawać stypendia pracownikom administracji publicznej posiadającym szczególnie wysokie kompetencje z obszaru technologii informatycznych i bezpieczeństwa teleinformatycznego,
- stypendia polegają na przyznawaniu środków finansowych,
- minister właściwy do spraw cyfryzacji w drodze rozporządzenia określi szczegółowe warunki i tryb przyznawania stypendiów oraz ich wysokość, mając na uwadze zapewnienie stosownych dodatkowych motywacyjnych dla specjalistów spełniających najwyższe kryteria fachowości w zakresie technologii informatycznych oraz bezpieczeństwa teleinformatycznego.

Następnie w odpowiednim rozporządzeniu, należałoby rozważyć wskazanie między innymi, iż:

- stypendium jest przyznawane w trybie konkursu ogłaszanego przez ministra właściwego do spraw cyfryzacji,
- ogłoszenie o konkursie zawiera informacje o: (1) przedmiocie konkursu, (2) terminie i miejscu składania wniosków, (3) warunkach udziału w konkursie, (4) procedurze i terminie rozstrzygnięcia konkursu,
- do ogłoszenia konkursu załącza się: (1) regulamin konkursu, (2) wzory formularza wniosku zgłoszeniowego, (3) wzór umowy stypendialnej,

- ogłoszenie o konkursie jest publikowane w Biuletynie Informacji Publicznej na stronie ministra właściwego do spraw cyfryzacji,
- wniosek o stypendium podlega ocenie formalnej i merytorycznej, zgodnie z wymogami określonymi we właściwym regulaminie konkursu,
- minister właściwy do spraw cyfryzacji może powierzyć opiniowanie wniosków, proponowanie wysokości oraz warunków stypendium powołanej przez siebie komisji,
- minister właściwy do spraw cyfryzacji przyznaje stypendium wnioskodawcom wybranym w konkursie,
- z osobą, której przyznano stypendium zawierana jest umowa stypendialna,
- umowa stypendialna stanowi podstawę wypłaty stypendium i określa m.in.: (1) obowiązki stypendysty i ministra, (2) wysokość stypendium oraz terminy i sposób płatności.

Omawiane rozporządzenie ministra właściwego do spraw cyfryzacji mogłoby również zawierać ogólnikowy opis obszaru kompetencji, jakie powinien posiadać wnioskodawca oraz cel programu stypendialnego.

Szczegółowe warunki jakie powinien spełniać wnioskodawca oraz kryteria oceny wniosków – wyłonienia zwycięzców konkursu, mogłyby natomiast zostać zawarte w regulaminie konkursu. Pozwoliłoby to na elastyczne przygotowywanie każdej edycji konkursu tak, aby bez potrzeby dokonywania zmian w przepisach prawa powszechnie obowiązującego, dostosowywać cele, wymogi oraz zobowiązania stypendystów do aktualnych potrzeb administracji publicznej i uwarunkowań z obszaru technologii informatycznych oraz bezpieczeństwa teleinformatycznego.

Wypłata świadczeń pieniężnych stypendystom zatrudnionym w administracji państwowej, zarówno w ramach korpusu służby cywilnej jaki poza tą strukturą, wydaje się być neutralna z perspektywy przepisów regulujących zasady wynagradzania.

Jednocześnie, celowym wydaje się również rozważenie dokonani a nowelizacji ustawy o podatku dochodowym od osób fizycznych poprzez dodanie w art. 21 ust. 1 odpowiedniego zwolnienia przedmiotowego obejmującego świadczenia pieniężne z programu stypendialnego „Złota Setka”.

6. Analiza ekonomiczna – luka płacowa w administracji w obszarze bezpieczeństwa IT

Cele programu „Złota setka” obejmują:

- Utrzymanie długoterminowego zatrudnienia najlepiej wykwalifikowanych pracowników z obszaru bezpieczeństwa IT w administracji.
- Zwiększenie poziomu motywacji i zaangażowania tych pracowników.
- Poszerzenie zakresu ich obowiązków i umożliwienie ich interwencji w przypadku poważnych incydentów w systemach teleinformatycznych administracji rządowej.

Realizacja celów programu wymaga zapewnienia pracownikom biorącym w nim udział konkurencyjnych wynagrodzeń – porównywalnych z otrzymywanymi w sektorze prywatnym. Oszacowania potrzeb w tym zakresie dokonano w oparciu o raporty płacowe dotyczące zarówno administracji publicznej jak sektora prywatnego. Obecnie Ministerstwo Cyfryzacji nie dysponuje bazą wiedzy w zakresie kompetencji i wynagrodzeń pracowników zajmujących się bezpieczeństwem IT w administracji publicznej, stąd niemożliwe jest przeprowadzenie analizy w oparciu o dane

rzeczywiste. Wydaje się jednak, że uzyskany poziom dokładności jest wystarczający na obecnym etapie przygotowania programu.

Szacunki poziomu wynagrodzeń, jakie obecnie otrzymują kandydaci do udziału w programie „Złota setka" w administracji publicznej dokonano w oparciu o Wynagrodzenia w administracji publicznej w 2017 roku, opracowanego przez Sedlak & Sedlak. Według tego raportu ogólna mediana wynagrodzeń w działach informatycznych wynosiła w 2017 roku 4 900 złotych[15]. Dla potrzeb niniejszej analizy posłużono się danymi dotyczącymi stanowisk w zakresie bezpieczeństwa IT w jednostkach administracji, które potencjalnie zostaną objęte programem – administracji rządowej i wielkich instytucjach. Zestawienie poziomów wynagrodzeń przedstawia tabela poniżej.

Tabela 4. Poziom obecnych wynagrodzeń kandydatów do programu Złota setka (zł brutto miesięcznie)

Stanowisko	Komentarze	Próba w badaniu	Mediana administracja
Administrator sieci informatycznej	wynagrodzenie całkowite	31	**4 094**
Administrator systemów IT	wynagrodzenie całkowite	31	**5 200**
Informatyk (stanowisko ogólne)	administracja rządowa	65	**3 966**
Informatyk (stanowisko ogólne)	wielka instytucja (1000 i więcej zatrudnionych)	76	**4 038**

Źródło: opracowanie własne na podstawie raportu Wynagrodzenia w administracji publicznej w 2017 roku

Na podstawie analizy danych średnie wynagrodzenie stanowiące podstawę do wyliczenia wymaganej wartości stypendium oszacowano obecnie na **4 325 złotych** brutto miesięcznie[16].

Wynagrodzenie to odniesiono do wynagrodzeń uzyskiwanych przez specjalistów w zakresie bezpieczeństwa IT w sektorze prywatnym. W celu ustalenia poziomu wynagrodzeń posłużono się również danymi firmy Sedlak & Sedlak[17]. Zgodnie z danymi na luty 2018 roku mediana wynagrodzeń w gospodarce na stanowisku specjalista ds. bezpieczeństwa informatycznego wynosiła **7 852 złote** brutto miesięcznie natomiast najlepiej wynagradzani pracownicy[18] otrzymywali co najmniej **10 811 złotych** brutto miesięcznie. W analizie przeprowadzono symulacje potrzeb zarówno przy założeniu wielkości stypendium odpowiadającemu zrównaniu płac w administracji do poziomu mediany jak również ze względu na wysoki poziom oczekiwań dla kandydatów do poziomu najwyżej opłacanych specjalistów.

W przypadku założenia zrównania przeciętnego wynagrodzenia w administracji należy oszacować koszt miesięczny dla każdego z pracowników na około **3 500 złotych** miesięcznie brutto, a w przypadku dążenia do najwyższych standardów rynkowych na **6 500 złotych** brutto miesięcznie. Obie kwoty nie uwzględniają potencjalnego kosztu ubezpieczenia społecznego po stronie pracodawcy. Obie kwoty oszacowano przy założeniu obciążenia podatkowego pracowników zgodnie z obowiązującymi zasadami naliczania podatku dochodowego od osób fizycznych oraz ubezpieczeń społecznych płaconych przez pracowników. Podsumowanie wartości prezentuje tabela poniżej.

[15] https://www.crn.pl/aktualnosci/zarobki-it-w-administracji
[16] Średnia arytmetyczna wielkości z tabeli powyżej
[17] https://wynagrodzenia.pl/moja-placa/ile-zarabia-specjalista-ds-bezpieczenstwa-informatycznego
[18] IV kwartyl – 25% najlepiej wynagradzanych pracowników

Tabela 5. Proponowane wartości stypendiów wypłacanych w ramach programu

Scenariusz	Różnica w stosunku do płacy rynkowej (zł/mc)	Proponowana wartość stypendium (zł/mc)	Korzyść netto dla pracownika (zł/mc)	Koszt jednostkowy po stronie administracji (zł/mc)
Wariant 1 Wyrównanie do poziomu rynkowego	3 528	**3 500**	2 520	4 223
Wariant 2 Wyrównanie do poziomu wynagrodzeń najwyższych	6 487	**6 500**	4 400	7 843

Źródło: opracowanie własne

Koszt programu dla administracji rządowej obejmie koszty wypłaty stypendiów oraz obsługi programu. Szacunkowo dla 100 osób objętych programem można te koszty oszacować na około **5 500 000 złotych** w przypadku scenariusza pierwszego oraz ponad **10 160 000 złotych** w przypadku scenariusza zakładającego uzyskanie wynagrodzeń na poziomie najwyższych wynagrodzeń rynkowych. Metodę wyliczenia kosztów rocznych przedstawiono w tabeli poniżej. Należy zauważyć, iż w przypadku uzyskania zwolnienia z podatku dochodowego dla stypendystów możliwe byłoby ograniczenie nakładów ze strony budżetu centralnego o kwotę **1 500 000 – 3 000 000 złotych rocznie.**

Tabela 6. Prognoza kosztów programu Złota Setka w pierwszym roku funkcjonowania

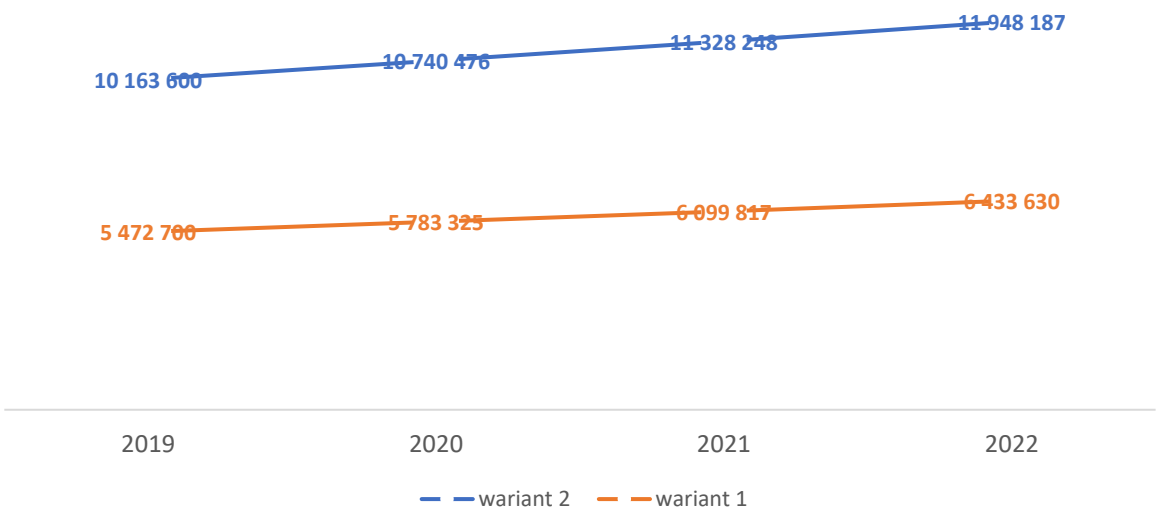
Scenariusz	Koszt jednostkowy dla Skarbu Państwa	Liczba osób objętych programem	Roczne koszty stypendiów	Koszty obsługi (8% rocznie)	Łączny koszt
Wariant 1 **Wyrównanie do poziomu rynkowego**	4 223	100	5 067 300	405 400	**5 472 700**
Wariant 2 **Wyrównanie do poziomu wynagrodzeń najwyższych**	7 843	100	9 410 700	752 900	**10 163 600**

Źródło: opracowanie własne

W kolejnych latach należy spodziewać się wzrostu kosztów realizacji programu ze względu na konieczność waloryzacji płac w odniesieniu do warunków rynkowych. Poniżej przedstawiono prognozę kosztów programu w okresie 4 lat (2019-2022) przy założeniu wzrostu wynagrodzeń zgodnie z prognozą wzrostu wynagrodzeń i inflacji zawartą w dokumencie *„Zaktualizowane warianty rozwoju gospodarczego Polski, o których mowa w Podrozdziale 7.4 Założenia do analizy finansowej – Wytycznych w zakresie zagadnień związanych z przygotowaniem projektów inwestycyjnych, w tym*

projektów generujących dochód i projektów hybrydowych na lata 2014-2020” wariant podstawowy wersja z dnia 16 sierpnia 2018 r.

Wykres 1. Prognoza kosztów programu Złota Setka w latach 2019-2022



Źródło: opracowanie własne

Łącznie w okresie 4 letnim szacowane koszty realizacji programu wyniosłyby od 23,8 miliona złotych w wariancie wyrównania wynagrodzeń do przeciętnych poziomów rynkowych do 44,2 milionów złotych w przypadku ustanowienia stypendiów na poziomie najwyższych wynagrodzeń w branży.

7. Zasady tworzenia i sposób umocowania programu w budżecie państwa

Program „Złota Setka” powinien być programem zarządzanym centralnie. Instytucją zarządzającą powinno być Ministerstwo Cyfryzacji jako organ koordynujący politykę cyberbezpieczeństwa RP.

Program „Złota Setka” będzie wieloletnim programem stypendialnym. Dodatkowe wynagrodzenie będzie wypłacane z budżetu państwa zarządzanego centralnie przez Ministerstwo Cyfryzacji (dysponenta budżetu) dla pracowników innych urzędów centralnych. Wynagrodzenie miałoby formę stypendium, przy czym formuła ta wymaga dopracowania od strony prawnej, gdyż obecnie brak jest odpowiednika programu w praktyce funkcjonowania administracji w Polsce.

W budżecie państwa stosuje się podział budżetu państwa na części budżetowe, które odpowiadają organom władzy publicznej, kontroli państwowej, sądom, trybunałom i innym organom, których projekty budżetu włączane są przez Ministra Finansów do projektu ustawy budżetowej, oraz administracji rządowej (art. 114 ust. 1 UFP). Odrębne części budżetowe tworzy się dla poszczególnych działów administracji rządowej oraz dla urzędów nadzorowanych przez Prezesa Rady Ministrów (art. 114 ust. 1 in fine UFP). W przypadku programu „Złota Setka” należałoby udostępnić środki na finansowanie programu i jego wdrożenie Ministrowi właściwemu ds. cyfryzacji.

Zwracamy uwagę, iż obecnie nie istnieją prawne mechanizmy umiejscowienia programu w budżecie Państwa. Brak jest zasad opisanych w prawie dotyczących ustanowienia stypendiów dla osób dorosłych na poziomie administracji centralnej. Pewnym precedensem w tym zakresie są stypendia dla olimpijczyków w ramach paragrafu 325 klasyfikacji budżetowej. Jednak na obecnym etapie nie ma możliwości zastosowania takiego rozwiązania w ramach klasyfikacji paragrafów budżetu – paragraf 325 wymagałby modyfikacji w tym zakresie i uwzględnienia dodatkowej grupy stypendystów.

8. Zasady użycia specjalistów będących beneficjentami programu

Specjaliści uczestniczący w programie będą mieli obowiązek wspierania administracji (MC i innych jednostek administracji rządowej do szczebla wojewódzkiego) w przypadku poważnych incydentów w systemach teleinformatycznych administracji rządowej. Przez poważny incydent rozumie się zgodnie z zapisami dokumentu Krajowe Ramy Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017-2022 - incydent lub grupę incydentów, które powodują lub mogą spowodować znaczną szkodę dla bezpieczeństwa publicznego, interesów międzynarodowych RP, w tym interesów gospodarczych, poziomu zaufania do instytucji publicznych, swobód obywatelskich lub zdrowia obywateli RP.

Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa definiuje incydent poważny jako *„incydent, który powoduje lub może spowodować poważne obniżenie jakości lub przerwanie ciągłości świadczenia usługi kluczowej*". Przy czym usługą kluczową jest każda usługa, która ma kluczowe znaczenie dla utrzymania krytycznej działalności społecznej lub gospodarczej i jest wymieniona w wykazie usług kluczowych[19]. Zgodnie z zapisami Ustawy podmiot publiczny jest zobowiązany do zarządzania incydentami w zakresie cyberbezpieczeństwa, w tym zgłoszenia wystąpienia incydentu w ciągu 24 godzin od jego wystąpienia oraz zapewnienia obsługi incydentu[20].

Podmiot taki wraz ze zgłoszeniem wystąpienia incydentu powinien również wskazać na potrzeby w zakresie specjalistów cyberbezpieczeństwa i wskazać na ich specjalizacje, zapotrzebowanie na pracę i szacunkowy czas niezbędnego oddelegowania.

Identyfikacja potrzeb w zakresie wykorzystania specjalistów korzystających z programu „Złota Setka"

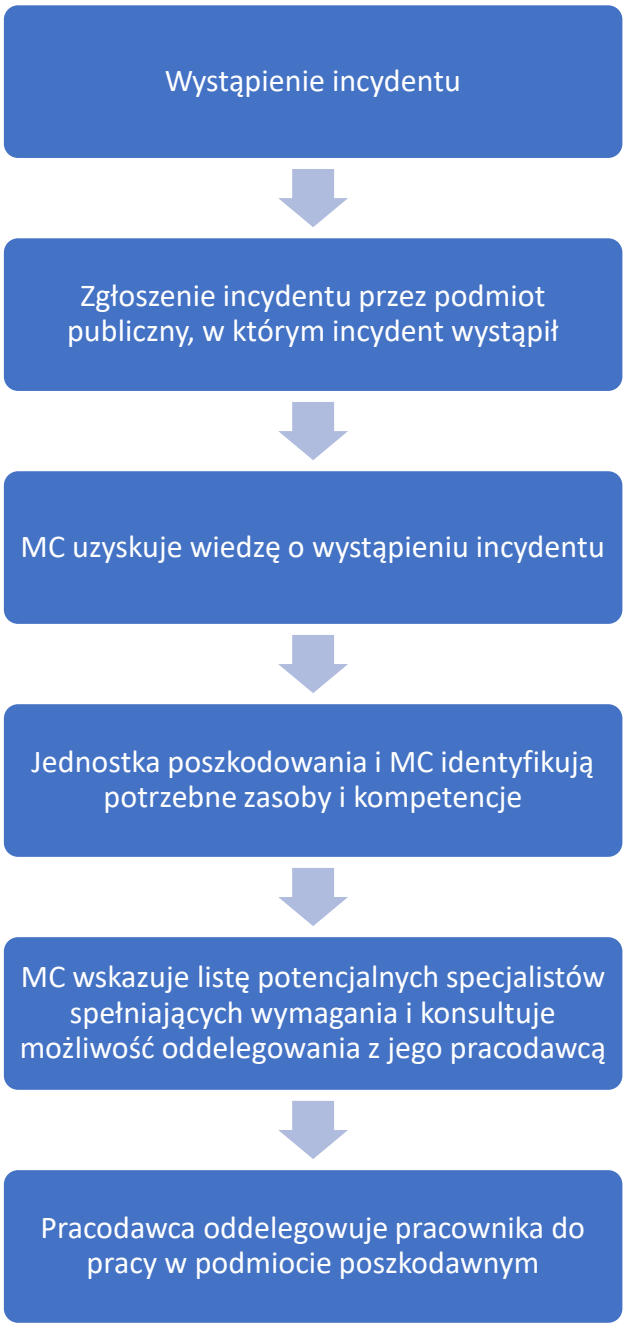
Specjaliści będący beneficjentami programu będą oddelegowani do pracy przez pracodawców za pośrednictwem Ministerstwa Cyfryzacji na podstawie umowy stypendialnej. Ministerstwo Cyfryzacji na podstawie posiadanej wiedzy o beneficjentach programu wskaże osoby spełniające potrzeby w zakresie obsługi incydentu.

Ministerstwo Cyfryzacji powinno decydować o udzieleniu danego specjalisty podmiotowi poszkodowanemu oraz skali i okresie oddelegowania zasobów do wsparcia obsługi incydentu po konsultacjach z podmiotem poszkodowanym oraz pracodawcami oddelegowanych specjalistów.

Schemat obsługi incydentów w systemach teleinformatycznych administracji rządowej przedstawia schemat poniżej.

[19] Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa Artykuł 1.
[20] Tamże, rozdział 5.

Rysunek 3. Schemat użycia specjalistów



Źródło: opracowanie własne

Jednocześnie obecny stan prawny bardzo ogranicza możliwości w zakresie delegowania pracowników, co negatywnie wpływa na możliwości ich wykorzystania do wspierania innych instytucji w trakcie incydentów.

Delegowanie członków korpusu służby cywilnej

Zagadnienie delegowania członków korpusu służby cywilnej regulują przepisy art. 62 do 66 ustawy z dnia 21 listopada 2008 roku o służbie cywilnej, przy czym z punktu widzenia niniejszego opracowania znaczenie mają zasady określone w art. 62, 63 oraz 64 przedmiotowej ustawy.

Stosownie do treści art. 62 ustawy o służbie cywilnej, jeżeli jest to uzasadnione potrzebami urzędu, dyrektor generalny urzędu może w każdym czasie przenieść urzędnika służby cywilnej na inne

stanowisko w tym samym urzędzie w tej samej lub w innej miejscowości, uwzględniając jego przygotowanie zawodowe. Przeniesienia urzędnika służby cywilnej na inne stanowisko w tym samym urzędzie do innej miejscowości nie można dokonać bez zgody urzędnika służby cywilnej - kobiety w ciąży lub osoby będącej jedynym opiekunem dziecka w wieku do lat piętnastu. Nie można także dokonać takiego przeniesienia, w przypadku gdy stoją temu na przeszkodzie szczególnie ważne względy osobiste lub rodzinne urzędnika. Przeniesienia urzędnika służby cywilnej na inne stanowisko w tym samym urzędzie do innej miejscowości znacznie oddalonej od dotychczasowego miejsca pracy urzędnika bez jego pisemnej zgody można dokonać nie częściej niż raz na dwa lata.

Cechą charakterystyczną możliwości przeniesienia służbowego ustanowionej w powyższym przepisie prawa jest, poza pewnymi wyjątkami, brak konieczności uzyskania zgody przenoszonego pracownika. Istotny jest natomiast czynnik w postaci potrzeb urzędu. Potrzeba urzędu jest tu zasadniczą podstawą przeniesienia, ale przyjmuje się, że musi ona być realna, konkretna i wskazywać, dlaczego na danym stanowisku urzędnik nie może być już zatrudniony. Przyczyny te muszą jednak leżeć po stronie urzędu (np. kwestie organizacyjne, budżetowe, zmiany przepisów, reorganizacja). Elementem istotnym jest też kwestia przygotowania zawodowego. Chodzi o to, by urzędnik przenoszony na inne stanowisko pracy dysponował odpowiednimi kwalifikacjami dającymi rękojmię prawidłowego wykonywania zadań na powierzonym stanowisku. W ramach wspominanych kwalifikacji istotne znaczenie ma też doświadczenie zawodowe i umiejętności nabyte w ciągu lat pracy. Dodatkowo, gdy przenoszona ma być urzędniczka-kobieta w ciąży, przeniesienie ma dotyczyć urzędnika, który jest jedynym opiekunem dziecka w wieku do 15 lat lub wtedy, gdy przeniesienie następuje do miejscowości znacznie oddalonej od dotychczasowego miejsca pracy urzędnika, wymagana jest zgoda przenoszonego urzędnika.

Art. 63 ustawy o służbie cywilnej stanowi natomiast, że jeżeli przemawia za tym interes służby cywilnej, Szef Służby Cywilnej może przenieść urzędnika służby cywilnej do innego urzędu w tej samej miejscowości, a jeżeli przemawia za tym szczególny interes służby cywilnej, Szef Służby Cywilnej może przenieść urzędnika służby cywilnej do innego urzędu w innej miejscowości na okres nie dłuższy niż 2 lata, a ponadto przeniesienie takie może nastąpić najwyżej dwa razy w czasie trwania stosunku pracy urzędnika służby cywilnej. Przeniesienie takie nie może nastąpić bez zgody urzędnika służby cywilnej - kobiety w ciąży lub osoby będącej jedynym opiekunem dziecka w wieku do lat piętnastu. Nie można także dokonać takiego przeniesienia w przypadku, gdy stoją temu na przeszkodzie szczególnie ważne względy osobiste lub rodzinne urzędnika.

Odnośny przepis reguluje zasady przenoszenia urzędników ze względu na interes służby cywilnej. Jeżeli bowiem przemawia za tym interes służby cywilnej, Szef Służby Cywilnej może przenieść urzędnika służby cywilnej do innego urzędu w tej samej miejscowości. Pojęcie interesu służby cywilnej odnosi się przy tym do służby jako takiej, a nie interesów poszczególnych urzędów. Przy tym przeniesieniu nie ma ram czasowych. Może być to zarówno przeniesienie czasowe, jak i stałe. Przeniesienie to może także następować wielokrotnie podczas trwania zatrudnienia.

Szef Służby Cywilnej może także, jeżeli przemawia za tym szczególny interes służby cywilnej, przenieść urzędnika służby cywilnej do innego urzędu w innej miejscowości na okres nie dłuższy jednak niż 2 lata. Przeniesienie takie może nastąpić najwyżej dwa razy w czasie trwania stosunku pracy urzędnika służby cywilnej. Analogicznie jak w przypadku art. 62, niektóre przypadki przeniesienia urzędnika wymagają jego zgody, a dotyczy to urzędnika – kobiety w ciąży lub osoby będącej jedynym opiekunem dziecka w wieku do lat 15. Nie można także dokonać takiego przeniesienia, jeżeli stoją temu na przeszkodzie szczególnie ważne względy osobiste lub rodzinne urzędnika.

Wreszcie możliwe jest przeniesienie urzędnika służby cywilnej oraz pracownika służby cywilnej do innego urzędu, także w innej miejscowości, na jego wniosek lub za jego zgodą (vide: art. 64 ustawy o służbie cywilnej). Przeniesienia takiego dokonuje dyrektor generalny urzędu, w którym urzędnik służby cywilnej oraz pracownik służby cywilnej ma być zatrudniony, w porozumieniu z dyrektorem generalnym urzędu, w którym ma miejsce dotychczasowe zatrudnienie.

Dla ważności przeniesienia z art. 64 ustawy o służbie cywilnej niezbędne jest wyrażenie zgody lub wniosek przenoszonego urzędnika lub pracownika służby cywilnej. Pracodawca nie może narzucić przejścia na tej podstawie. Podstawą przeniesienia jest porozumienie dyrektora generalnego urzędu dotychczasowego i dyrektora generalnego urzędy przyszłego (urzędu, w którym urzędnik służby cywilnej oraz pracownik służby cywilnej ma być zatrudniony). Omawiane przeniesienie skutkuje kontynuacją dotąd istniejącego stosunku pracy. Nie następuje zakończenie zatrudnienia i nie są wykonywane związane z tym czynności (np. wydanie świadectwa pracy), a dotychczasowy pracodawca zobowiązany jest do przekazania dokumentacji pracowniczej nowemu pracodawcy.

Delegowanie urzędników państwowych

Reguły delegowania urzędników państwowych niebędących członkami korpusu służby cywilnej określa przede wszystkim art. 10 ustawy z dnia 16 września 1982 roku o pracownikach urzędów państwowych. Z odnośnego przepisu prawa wynika przede wszystkim, że jeżeli wymagają tego potrzeby urzędu, urzędnikowi państwowemu można zlecić, na okres jednak nie dłuższy niż trzy miesiące w roku kalendarzowym, wykonywanie innej pracy niż określona jego w akcie mianowania lub w umowie o pracę, zgodnej z jego kwalifikacjami. Ponadto, w razie reorganizacji urzędu urzędnika państwowego mianowanego można przenieść na inne stanowisko służbowe, odpowiadające jego kwalifikacjom, jeżeli ze względu na likwidację stanowiska zajmowanego przez urzędnika nie jest możliwe dalsze jego zatrudnienie na tym stanowisku. Przepis ten przewiduje również, że w przypadku, gdy istnieją szczególne potrzeby urzędu, urzędnika państwowego mianowanego można przenieść na inne stanowisko, odpowiadające jednak jego kwalifikacjom urzędnika i równorzędne pod względem wynagrodzenia. Na wniosek natomiast urzędnika państwowego lub za jego zgodą, urzędnika można przenieść do pracy w innym urzędzie w tej samej lub innej miejscowości, a przeniesienia dokonuje kierownik urzędu, w którym urzędnik ten ma być zatrudniony, w porozumieniu z kierownikiem urzędu dotychczas zatrudniającego urzędnika. Ustawodawca przewidział również, że w uzasadnionych wypadkach urzędnik państwowy mianowany może być przeniesiony, na okres do sześciu miesięcy, do innego urzędu w tej samej lub innej miejscowości, do pracy zgodnej z posiadanymi kwalifikacjami, przy czym tego rodzaju przeniesienie dopuszczalne jest tylko raz na dwa lata.

Analogicznie jak w przypadku członków korpusu służby cywilnej, także w stosunku do pozostałych urzędników państwowych ustawodawca przewidział w niektórych przypadkach pewne ograniczenia w zakresie możliwości ich przenoszenia służbowego. Za niedopuszczalne, bez zgody urzędnika, jest czasowe przeniesienie do urzędu mającego siedzibę w innej miejscowości kobiety w ciąży lub urzędnika państwowego sprawującego opiekę nad dzieckiem w wieku do czternastu lat, a także w wypadkach, gdy stoją temu na przeszkodzie ważne względy osobiste lub rodzinne urzędnika.

Istotne jest również, że urzędnik państwowy nie może podejmować dodatkowego zatrudnienia bez uzyskania uprzedniej zgody kierownika urzędu, w którym jest zatrudniony. Urzędnik państwowy nie może też wykonywać zajęć, które pozostawałyby w sprzeczności z jego obowiązkami albo mogłyby wywołać podejrzenie o stronniczość lub interesowność (vide: art. 19 ustawy o urzędnikach państwowych).

Delegowanie innych pracowników

W zakresie pracowników urzędów państwowych niebędących członkami korpusu służby cywilnej ani urzędnikami państwowymi, zasady ich delegowania (a w zasadzie tzw. oddelegowania) określają przepisy Kodeksu pracy.

Możliwość czasowego oddelegowania pracownika do innej pracy przewiduje art. 42 § 4 Kodeksu pracy, w myśl którego wypowiedzenie dotychczasowych warunków pracy lub płacy nie jest wymagane w razie powierzenia pracownikowi, w przypadkach uzasadnionych potrzebami pracodawcy, innej pracy niż określona w umowie o pracę na okres nieprzekraczający 3 miesięcy w roku kalendarzowym, jeżeli nie powoduje to obniżenia wynagrodzenia i odpowiada kwalifikacjom pracownika. A zatem pracodawca mający uzasadnione potrzeby może skierować swego pracownika do innej pracy na czas określony, tj. do 3 miesięcy w roku. Należy zwrócić uwagę, że w praktyce pracodawca może powierzyć inną pracę na okres od 1 listopada 2017 roku do 31 marca 2018 roku. Ograniczenie czasowe dotyczy bowiem jednego roku kalendarzowego.

Każdorazowo praca do jakiej oddelegowany zostaje pracownik musi odpowiadać kwalifikacjom pracownika i nie powodować spadku jego wynagrodzenia. Powierzenie pracownikowi innej pracy ma formę polecenia pracodawcy i znajduje oparcie w art. 100 Kodeksu pracy. Pracodawca nie ma też obowiązku konsultowania zamiaru takiego oddelegowania pracownika z zakładową organizacją związkową reprezentującą prawa i interesy tego pracownika.

Co istotne, pracodawca może powierzyć pracownikowi inną pracę niż ustalona w umowie o pracę w razie istnienia uzasadnionych potrzeb. Mogą to być np. potrzeby organizacyjne lub techniczne wymagające skierowania do innej pracy określonych pracowników. Według Sądu Najwyższego użyte w art. 42 § 4 Kodeksu pracy określenie „uzasadnione potrzeby pracodawcy" oznaczają uzasadnione potrzeby zakładu pracy jako całości, a nie tylko komórki organizacyjnej, do pracy, w której pracownik został skierowany (wyrok SN z 8 sierpnia 1979 r., I PR 55/79, OSNC 1980/2/30).

Stosownie do postanowień art. 46 ustawy o pracownikach urzędów państwowych, przepisy art. 21-31 i 33 tejże ustawy stosuje się również do pracowników urzędów państwowych niebędących urzędnikami.

W kontekście delegowania tych pracowników pewne znaczenie może mieć art. 26 ustawy o pracownikach urzędów państwowych, zgodnie z którym:

- pracownikowi urzędu państwowego, delegowanemu służbowo do zajęć poza siedzibą urzędu, w którym jest zatrudniony, przysługują zwrot kosztów podróży, zakwaterowania oraz diety na zasadach stosowanych przy podróżach służbowych na obszarze kraju,
- pracownikowi urzędu państwowego przenoszonemu do pracy w innej miejscowości przysługują zwrot kosztów przeniesienia, diety, zwrot kosztów podróży oraz inne świadczenia,
- Rada Ministrów określiła, w drodze rozporządzenia, wysokość i warunki wypłacania odpowiednich świadczeń należnym pracownikom (vide: rozporządzenie Rady Ministrów z dnia 30 kwietnia 2002 roku w sprawie wysokości i warunków wypłacania świadczeń urzędnikom państwowym przeniesionym do pracy w innej miejscowości).

Wymaga podkreślenia, że niezależnie od przepisów Kodeksu pracy, w przypadku, gdy obie strony (pracownik i pracodawca) wyrażą zgodę, możliwe jest powierzenie innych obowiązków na dowolny czas. Najlepiej, aby zostało to uregulowane w formalny sposób, np. poprzez sporządzenie aneksu do umowy o pracę, który będzie zawierał dodatkowy zakres zadań. Zgodnie z orzecznictwem Sądu Najwyższego przyjmuje się, że w przypadku gdy po upływie trzymiesięcznego okresu pracownik nadal

wykonuje obowiązki innego pracownika i stan ten akceptuje, można uznać, że doszło w sposób dorozumiany do zawarcia porozumienia zmieniającego warunki pracy (por. uzasadnienie wyroku SN z 13 grudnia 2005 r., sygn. akt II PK 103/05).

Powyższa instytucja znajduje jedynie zastosowanie w przypadku czasowego oddelegowania pracownika do innych zadań w ramach struktury tego samego pracodawcy, co czyni ją mało użyteczną przy realizacji omawianego projektu stypendialnego.

Podsumowanie

Wydaje się, że w kontekście wizji i prawdopodobnych potrzeb Ministerstwa Cyfryzacji w zakresie możliwości wykorzystania pracy beneficjentów stypendium, brak jest w aktualnie obowiązujących przepisach adekwatnych regulacji prawnych, które dodatkowo miałyby tożsame dla trzech przedstawionych powyżej grup pracowników.

Odnośnie delegowania pracowników - członków korpusu służby cywilnej, w aktualnym stanie prawnym, potencjalnym rozwiązaniem wydaje się być skorzystanie z instytucji przeniesienia urzędnika na zasadach wyrażonych w art. 63 ust. 1 ustawy o służbie cywilnej. Dotyczy to jednak tylko oddelegowania do pracy w tej samej miejscowości i wymaga zaangażowania Szefa Służby Cywilnej.

Alternatywą jest przeniesienie urzędnika uregulowane w art. 64 ustawy o służbie cywilnej. Za każdym razem wymaga jednak to porozumienia pomiędzy dyrektorem generalnym urzędu dotychczasowego oraz dyrektorem generalnym urzędu docelowego (oraz oczywiście zgody pracownika). Instytucja ta została jednak stworzona w celu trwałego przejścia pracownika do nowego urzędy, a nie czasowego oddelegowania. Stąd też, w praktyce każdorazowe przeniesienie wymaga możliwości stworzenia dodatkowego etatu oraz posiadania odpowiednich źródeł finansowania zarówno w urzędzie docelowym (tu Ministerstwie Cyfryzacji, do którego czasowo miałby przejść pracownik) jak i w urzędzie macierzystym (po tym jak pracownik miałby, po zlikwidowaniu etatu, wrócić do swojego poprzedniego miejsca zatrudnienia).

Oddelegowanie pracownika - urzędnika państwowego niebędącego członkiem korpusu służby cywilnej może nastąpić w drodze przeniesienia na mocy art. 10 ust. 2 ustawy o urzędnikach państwowych (podobnego w swoich założeniach i wadach do omówionego wyżej art. 64 ustawy o służbie cywilnej) lub art. 10 ust. 3 ustawy o urzędnikach państwowych. Przy czym, w tym drugim przypadku, przeniesienie takie dopuszczalne jest tylko raz na dwa lata, a zatem wydaje się być trudne do pogodzenia z założeniami stypendium.

Odnośnie pracowników podlegających stricte pod kodeks pracy, brak jest odpowiednich norm prawnych umożliwiających ex lege utrzymanie stosunku pracy i czasowe przenoszenie pracownika pomiędzy urzędami administracji państwowej. Wymagałoby to skorzystania z instytucji urlopu bezpłatnego w macierzystym urzędzie i nawiązania nowego stosunku pracy w urzędzie docelowym. Wszelkie uzgodnienia w tym zakresie musiałyby przybrać formę umów – porozumień pomiędzy pracodawcami a pracownikiem.

Wydaje się więc, że na dzień dzisiejszy nie istnieją efektywne, systemowe mechanizmy, które pozwoliłby na oddelegowanie pracowników objętych programem „Złota Setka” do obsługi incydentów w innych podmiotach niż są zatrudnieni.

Warto rozważyć podejście bardziej proaktywne w zakresie obsługi incydentów cyberbezpieczeństwa. Działania proaktywne koncentrują się na przygotowaniu mechanizmów odpowiedzi na możliwy incydent, których elementem jest również kompetentny personel. Należy zakładać, że w sytuacji

kryzysowej brak takiego personelu mógłby okazać się paraliżujący, stąd pozyskanie odpowiednich kompetencji w zakładanym czasie jest kluczowe z punktu widzenia podmiotów obsługujących incydent. Wymaga to przygotowania mechanizmów, procedur, treningów i wszelkich nakładów organizacyjnych i prawnych niezbędnych do tego aby specjaliści innych obszarów mogli brać udział w reagowaniu na incydenty w innych podmiotach.

Dodatkowo z punktu widzenia bezpieczeństwa niesłychanie ważne jest aby kluczowe procesy i usługi stale wykazywały zakładany poziom dostępności. Może to oznaczać, że istotnym elementem tego wymagania jest posiadanie odpowiednich kompetencji personelu, który je obsługuje. Specjaliści uczestniczący w programie powinni również wspierać całość administracji w obszarach, dla których brak jest odpowiedniego personelu i gdzie niedobór kadry może zatrzymać kluczowy proces lub obniżyć jego dostępność do nieakceptowalnego poziomu (na przykład grożącemu wystąpieniu sytuacji kryzysowej).

Wydaje się, że w tej sytuacji można rozważyć powołanie Centrum Usług Wspólnych (CUW) w obszarze cyberbezpieczeństwa, które zatrudniałoby stypendystów programu „Złota Setka”. Takie rozwiązanie pozwoliłoby na rozwiązanie problemów związanych z delegowaniem pracowników i jednocześnie umożliwiło stworzenie stałego zasobu kadrowego w obszarze bezpieczeństwa systemów i usług IT w administracji centralnej.

9. Wnioski i rekomendacje

Program „Złota Setka” będzie wieloletnim programem stypendialnym. Dodatkowe wynagrodzenie będzie wypłacane z budżetu państwa za pośrednictwem Ministerstwa Cyfryzacji jako dysponenta środków dla pracowników innych urzędów centralnych. Program taki ma na celu utrzymanie zatrudnienia wysokiej jakości specjalistów w zakresie cyberbezpieczeństwa w administracji publicznej. Obecnie poziom wynagrodzeń takich specjalistów w sektorze publicznym znacząco odbiega od realiów rynkowych, co przyczynia się do silnej rotacji pracowników działów IT oraz odpływu najlepszych specjalistów do sektora prywatnego. Program „Złota Setka” umożliwiłby również stworzenie trwałego zasobu kadrowego wspierającego obsługę poważnych incydentów w zakresie cyberbezpieczeństwa, do jakich może dochodzić w przyszłości w podmiotach publicznych.

Program wydaje się dobrze odpowiadać na postawione przed nim cele w zakresie utrzymania pracowników IT w jednostkach administracji, jednak ze względu na poważne ograniczenia prawne w zakresie delegacji pracowników ich wykorzystanie w zakresie wsparcia w przypadku poważnych incydentów cyberbezpieczeństwa w innych podmiotach będzie bardzo trudne.

W ramach przeprowadzonej analizy zidentyfikowano szereg specjalizacji z obszaru informatyki i telekomunikacji, specjaliści których powinni być kwalifikowani do programu i uzyskać możliwość korzystania ze stypendium. Zakresy kompetencji zidentyfikowano na podstawie analizy modelu bezpieczeństwa informatycznego oraz obszarów wskazanych w dokumencie „Krajowe Ramy Polityki Krajowe Ramy Polityki Krajowe Ramy Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017-2022”.

Przeprowadzona w ramach opracowania analiza prawna wskazuje na brak obecnie uregulowań pozwalających na realizację programu „Złota Setka”. Konieczne jest jego ustawowe umocowanie, ponieważ nie istnieją obecnie adekwatne przepisy umożliwiające wypłatę stypendiów dla pracowników administracji.

Wdrożenie programu wymaga regulacji prawnej na poziomie ustawy, ze względów praktycznych najlepszym rozwiązaniem wydaje się dokonanie takiej regulacji poprzez nowelizację ustawy o krajowym systemie cyberbezpieczeństwa.

Najbardziej adekwatnym modelem zorganizowania postępowania związanego z procedowaniem i przyznawaniem zakładanych świadczeń motywacyjnych (stypendiów) w ramach programu wydaje się metoda konkursowa. Wymaga ona co prawda i tak umocowania na poziomie przepisów prawa powszechnie obowiązującego (niezbędnym jest przynajmniej określone źródła finansowania i podstawy prawnej do zorganizowania programu) oferuje jednak równocześnie stosunkowo wysoką elastyczność w zakresie rekrutacji specjalistów do programu.

Założono, że kandydatów do stypendiów będą zgłaszać kierownicy jednostek w odpowiedzi na nabór konkursowy ogłaszany przez Ministerstwo Cyfryzacji. Minister właściwy do spraw cyfryzacji będzie ogłaszać konkursy zgodnie z umocowaniem ustawowym i wydanym przez siebie rozporządzeniem. Zasady naboru kandydatów w sposób ogólny zostaną wskazane w ramach rozporządzenia natomiast szczegółowe zasady i kryteria naboru kandydatów będą określane w regulaminie konkursu. Każdy z konkursów będzie określać liczbę stypendystów oraz ich strukturę (liczbę miejsc w ramach poszczególnych specjalizacji branżowych w obszarze cyberbezpieczeństwa).

Każdy z pracowników, aby wziąć udział w konkursie musiałby spełnić, co najmniej następujące warunki:

- Posiadane kompetencje w zakresie co najmniej jednej ze wskazanych w regulaminie konkursu specjalizacji w zakresie bezpieczeństwa informatycznego.
- Zatrudnienie na stanowisku informatycznym i wykonywanie obowiązków związanych z jedną ze wskazanych specjalizacji.
- Potwierdzenie posiadanych kompetencji ważnym certyfikatem z proponowanej w niniejszym opracowaniu listy.

Koszty realizacji programu oszacowano wstępnie w na kwotę od 23,8 miliona złotych w wariancie wyrównania wynagrodzeń do przeciętnych poziomów rynkowych do 44,2 milionów złotych w przypadku ustanowienia stypendiów na poziomie najwyższych wynagrodzeń w branży. Warto zauważyć, iż istnieje ustawowa możliwość zwolnienia stypendystów z podatku od dochodów osobistych (PIT), co znacząco obniżyłoby koszty programu (przynajmniej o 20%).

Zwracamy uwagę, iż obecnie Ministerstwo Cyfryzacji nie posiada wiedzy w zakresie kompetencji oraz stanu zasobów kadrowych związanych z zapewnieniem cyberbezpieczeństwa zatrudnionych w administracji publicznej. Rekomendujemy więc opracowanie stosownej bazy danych pracowników IT podmiotów publicznych, co pozwoli na efektywną rekrutację do programu i zarządzanie zasobami w trakcie incydentów bezpieczeństwa.

Kluczowym problemem wymagającym rozwiązania jest sposób oddelegowywania pracowników korzystających ze stypendiów do obsługi incydentów w innych podmiotach publicznych. W dłuższej perspektywie wydaje się zasadnym rozważenie możliwości stworzenia Centrum Usług Wspólnych w obszarze obsługi administracji centralnej w zakresie cyberbezpieczeństwa.

10. Spis tabel

11. Spis wykresów i rysunków