Projekt z dnia 23 grudnia 2021 r.

R O Z P O R Z Ą D Z E N I E

R A D Y M I N I S T R Ó W

z dnia ……..

w sprawie wysokości świadczenia teleinformatycznego osób realizujących zadania z zakresu cyberbezpieczeństwa

Na podstawie art. 8 ust. 1 ustawy z dnia 2 grudnia 2021 r. o szczególnych zasadach wynagradzania osób realizujących zadania z zakresu cyberbezpieczeństwa (Dz. U. poz. 2333), zarządza się, co następuje:

§ 1. Rozporządzenie określa:

1) szczegółowe zadania z zakresu cyberbezpieczeństwa i podział ich na grupy;
2) doświadczenie zawodowe lub wymóg posiadania specjalistycznej wiedzy z zakresu cyberbezpieczeństwa wymagane do realizacji zadań z poszczególnych grup;
3) przedziały kwotowe wysokości świadczenia teleinformatycznego w związku z podziałem zadań z zakresu cyberbezpieczeństwa na grupy, o których mowa w pkt 1.

§ 2. Ustala się tabelę szczegółowych zadań z zakresu cyberbezpieczeństwa oraz doświadczenia zawodowego lub posiadania specjalistycznej wiedzy w zakresie cyberbezpieczeństwa, a także przedziały kwotowe wysokości świadczenia teleinformatycznego osób realizujących zadania z zakresu cyberbezpieczeństwa, stanowiącą załącznik do rozporządzenia.

§ 3. Rozporządzenie wchodzi w życie po upływie 5 dni od dnia ogłoszenia.

PREZES RADY MINISTRÓW

Załącznik do rozporządzenia Rady Ministrów z dnia……(poz. …)

Tabela szczegółowych zadań z zakresu cyberbezpieczeństwa oraz doświadczenia zawodowego lub posiadania specjalistycznej wiedzy w zakresie cyberbezpieczeństwa a także przedziały kwotowe wysokości świadczenia teleinformatycznego osób realizujących zadania z zakresu cyberbezpieczeństwa

<table>
<tr><th>Lp.</th><th>Doświadczenie zawodowe w realizacji zadań w zakresie cyberbezpieczeństwa, w latach</th><th colspan="2">Przedziały kwotowe wysokości świadczenia teleinformatycznego</th><th>Szczegółowe zadania</th><th>Wymóg posiadania specjalistycznej wiedzy w zakresie cyberbezpieczeństwa, o której mowa w poniższych dokumentach</th></tr>
<tr><td rowspan="3">1.</td><td>do 3 lat</td><td rowspan="3">2000</td><td>12000</td><td rowspan="3">Analiza szkodliwego oprogramowania
Badanie bezpieczeństwa, podatności i testowanie sprzętu lub oprogramowania
Ocena bezpieczeństwa systemów IT – w tym testy penetracyjne i audyty bezpieczeństwa
Prowadzenie specjalistycznych analiz cyberbezpieczeństwa i wykrywanie nowych podatności
Rozwijanie specjalistycznych narzędzi technicznych wspomagających realizację zadań z obszaru cyberbezpieczeństwa</td><td rowspan="3">CASP+, CCFE, CEH, CEH Master, CPENT, CSSLP, CHFI, CMFE, CPT, eCDFP, eCMAP, CISSP, GASF, GAWN, GCCC, GCDA, GCFA, GCPN, GCTI, GNFA, GPEN, GREM, GREM, GSAF, GSNA, GMOB, GSSP, GWAPT, GWEB, GXPN, LPT, OSCE3, OSCP, OSED, OSEP, OSEE, OSMR, OSWA, OSWE, OSWP,

PenTest+

lub w dokumencie potwierdzającym zajęcie pierwszego miejsca w:
Core NetWars Tournament[1],
Cyber Defense NetWars[2],
DFIR NetWars Tournament[3],
Grid NetWars Tournament[4],
ICS NetWars Tournament[5]</td></tr>
<tr><td>od 3 do 5 lat</td><td>18000</td></tr>
<tr><td>powyżej 5 lat</td><td>30000</td></tr>
<tr><td>2.</td><td></td><td></td><td></td><td></td><td></td></tr>
</table>

[1] https://www.sans.org/cyber-ranges/netwars-tournaments/core/
[2] https://www.sans.org/cyber-ranges/netwars-tournaments/cyber-defense/
[3] https://www.sans.org/cyber-ranges/netwars-tournaments/digital-forensics-incident-response/
[4] https://www.sans.org/cyber-ranges/netwars-tournaments/power-grid/
[5] https://www.sans.org/cyber-ranges/netwars-tournaments/industrial-control-system-security/

	do 3 lat	2000	12000	• Kierowanie jednostką organizacyjną przeznaczoną do realizacji zadań z zakresu cyberbezpieczeństwa z wyłączeniem kierownika podmiotu • Prowadzenie działań prewencyjnych zwiększających cyberbezpieczeństwo • Zaawansowana obsługa incydentów	BTL2, CASP+, CEH Master, CISM, CISSP, CPENT CySA+, GCCC, GCDA, GCIH, GCPM, GCSA, GDAT, GISP, GPYC, GSLC, GSOM, GSTRT, GXPN, GWEB, PenTest+, OSCP, OSEE, OSEP lub w dokumencie potwierdzającym zajęcie pierwszego miejsca w: • Core NetWars Tournament, • Cyber Defense NetWars, • DFIR NetWars Tournament, • Grid NetWars Tournament, • ICS NetWars Tournament
	od 3 do 5 lat		18000		
	powyżej 5 lat		25000		
3.	do 3 lat	2000	8000	• Analiza powłamaniowa • Badanie i ocena bezpieczeństwa rozwiązań ICT • Budowa i utrzymanie systemów monitorowania i detekcji incydentów oraz wsparcia funkcjonowania SOC • Kierowanie komórką organizacyjną przeznaczoną do realizacji zadań z zakresu cyberbezpieczeństwa • Korelacja danych, prowadzenie analiz lub tworzenie map sytuacyjnych • Monitorowanie zagrożeń cyberbezpieczeństwa i incydentów na poziomie krajowym • Prowadzenie analiz incydentów poważnych, powiązań pomiędzy incydentami oraz opracowywanie wniosków • Przyjmowanie zgłoszeń i obsługa incydentów poważnych	BTL1, BTL2, CAP, CASP+, CAWFE, CEH, CEH-Master, CISM, CCFE, CDRP, CFSR, CISSP, CHFI, CPENT, CSSLP, CNFE, CySA+, eCDFP, eCMAP, GCCC, GCDA, GCFA, GCFE, GCIH, GCSA, GISP, GMON, GNFA, GSAF, GSE, GSLC, GSOC, GSOM, GWEB, OSCP, OSEE, OSEP, PenTest+, Security+, SSCP lub w dokumencie potwierdzającym zajęcie pierwszego miejsca w: • Core NetWars Tournament, • Cyber Defense NetWars, • DFIR NetWars Tournament, • Grid NetWars Tournament, • ICS NetWars Tournament
	od 3 do 5 lat		12000		
	powyżej 5 lat		20000		

				• Reagowanie na incydenty oraz ich klasyfikacja • Szacowanie ryzyka w obszarze cyberbezpieczeństwa	
4.	do 3 lat	2000	6000	• Analiza i zarządzanie w zakresie reagowania na wykryte podatności sprzętu i oprogramowania • Koordynacja obsługi zgłoszonych incydentów • Obsługa zgłoszeń i analiza treści przypadków dystrybucji, rozpowszechniania lub przesyłania pornografii dziecięcej za pośrednictwem technologii informacyjno-komunikacyjnych • Opracowywanie i wdrażanie planów ciągłości działania i odbudowy oraz systemu zarządzania bezpieczeństwem informacji • Specjalistyczne zadania realizowane w ramach SOC lub NOC obejmujące: monitoring bezpieczeństwa (analiza i korelacja logów), identyfikację i wstępną obsługę incydentów	BTL1, BTL2, CASP+, CEH, CEH Master, CISSP, CPENT, CySA+, GCIH, GCDA, GDAT, GISP, GMON, GSLC, GSOC, MGT, OSCP, Security+, SSCP lub w dokumencie potwierdzającym zajęcie pierwszego miejsca w: • Core NetWars Tournament, • Cyber Defense NetWars, • DFIR NetWars Tournament, • Grid NetWars Tournament, • ICS NetWars Tournament
	od 3 do 5 lat		9000		
	powyżej 5 lat		15000		
5.	do 3 lat	2000	5000	• Nadzór nad procesem szacowania ryzyka w obszarze cyberbezpieczeństwa • Przygotowywanie rekomendacji, standardów i dobrych praktyk w zakresie cyberbezpieczeństwa w szczególności podnoszących poziom bezpieczeństwa systemów IT będących w dyspozycji podmiotów krajowego systemu cyberbezpieczeństwa	CAP, CASP+, CEH, CISA, CISSP, GISP, GSE, GSLC, GSNA, SSCP lub w dokumencie potwierdzającym zajęcie pierwszego miejsca w: • Core NetWars Tournament, • Cyber Defense NetWars, • DFIR NetWars Tournament, • Grid NetWars Tournament, • ICS NetWars Tournament
	powyżej 3 lat		8000		
	powyżej 5 lat		12000		
6.	do 3 lat	2000	4500	• Bieżące utrzymanie i rozwój własnych, istotnych systemów IT	BTL1, CASP+, CEH, CEH-Master, CISA, CPENT, CSSLP, CySA+, ITIL

	od 3 do 5 lat		6000	• Poszukiwanie znanych podatności sprzętu i oprogramowania w nadzorowanych systemach teleinformatycznych • Wstępna obsługa incydentów • Zabezpieczenie śladów cyfrowych • Rozpoznawanie zagrożeń cyberbezpieczeństwa	Managing Professional, OSCP, OSEE, OSEP, GBFA, GCIH, GOSI, GMON, PenTest+, Security+, SSCP lub w dokumencie potwierdzającym zajęcie pierwszego miejsca w: • Core NetWars Tournament, • Cyber Defense NetWars, • DFIR NetWars Tournament, • Grid NetWars Tournament, • ICS NetWars Tournament
	powyżej 5 lat		10500		
7.	do 3 lat	2000	6000	• Identyfikacja oraz prowadzenie postępowań wobec operatorów usług kluczowych • Nadzór nad podmiotami krajowego systemu cyberbezpieczeństwa • Nadzór nad podmiotami świadczącymi usługi z zakresu cyberbezpieczeństwa • Prowadzenie akcji podnoszących świadomość w obszarze cyberbezpieczeństwa w szczególności organizacja ćwiczeń i szkoleń • Prowadzenie analiz w zakresie funkcjonowania krajowego systemu cyberbezpieczeństwa w tym w zakresie rozwiązań prawnych, organizacyjnych, standardów oraz certyfikacji w obszarze cyberbezpieczeństwa wraz z przygotowywaniem projektów aktów normatywnych • Prowadzenie analiz w zakresie spełniania przez podmioty z sektora lub podsektora warunków kwalifikujących podmiot jako operatora usługi kluczowej	CASP+, CEH, CGAP, CIA, CISA, CISM, CISSP, GISP, GSLC, Security+ lub w dokumencie potwierdzającym zajęcie pierwszego miejsca w: • Core NetWars Tournament, • Cyber Defense NetWars, • DFIR NetWars Tournament, • Grid NetWars Tournament, • ICS NetWars Tournament
	powyżej 3 lat		8000		

				• Prowadzenie kontroli w podmiotach krajowego systemu cyberbezpieczeństwa, w tym w podmiotach świadczących usługi z zakresu cyberbezpieczeństwa • Współpraca krajowa lub międzynarodowa w obszarze cyberbezpieczeństwa	

Zestawienie wymienionych w tabeli certyfikatów:
BTL1 – Security Blue Team Level 1
BTL2 – Security Blue Team Level 2
CAP – Certified Authorization Professional
CASP+ – CompTIA Advanced Security Practitioner
CAWFE – Certified Advanced Windows Forensic Examiner
CCFE – Certified Computer Forensics Examiner
CCFE – Certified Computer Forensics Examiner
CDRP – Certified Data Recovery Professional
CEH – Certified Ethical Hacker
CEH Master – Certified Ethical Hacker Master
CFSR – Certified Forensic Security Responder
CGAP – Certified Government Auditing Professional
CHFI – Certified Hacking Forensic Investigator
CIA – Certified Internal Auditor
CISA – Certified Information Systems Auditor
CISM – Certified Information Security Manager
CISSP – Certified Information Systems Security Professional
CMFE – Certified Mobile Forensics Examiner
CNFE – Certified Network Forensics Examiner
CPENT – Certified Penetration Testing Professional
CPT – Certified Penetration Tester
CSSLP – Certified Secure Software Lifecycle Professional
CySA+ – CompTIA CySA+
eCDFP – eLearnSecurity Certified Digital Forensics Professional
eCDFP – eLearnSecurity Certified Digital Forensics Professional
eCMAP – eLearnSecurity Certified Malware Analysis Professional
GASF – GIAC Advanced Smartphone Forensics
GAWN – GIAC Assessing and Auditing Wireless Networks
GBFA – GIAC Battlefield Forensics and Acquisition
GCCC – GIAC Critical Controls Certification
GCDA – GIAC Certified Detection Analyst
GCFA – GIAC Certified Forensic Analyst
GCFE – GIAC Certified Forensic Examiner
GCIH – GIAC Certified Incident Handler
GCPM – GIAC Certified Project Manager
GCPN – GIAC Cloud Penetration Tester
GCSA – GIAC Cloud Security Automation
GCTI – GIAC Cyber Threat Intelligence

GDAT – GIAC Defending Advanced Threats
GISP – GIAC Information Security Professional
GMOB – GIAC Mobile Device Security Analyst
GMON – GIAC Continuous Monitoring Certification
GNFA – GIAC Network Forensic Analyst
GOSI – GIAC Open Source Intelligence
GPEN – GIAC Penetration Tester
GPYC – GIAC Python Coder
GREM – GIAC Reverse Engineering Malware
GSE – GIAC Security Expert
GSLC – GIAC Security Leadership
GSNA – GIAC Systems and Network Auditor
GSOC – GIAC Security Operations Certified
GSOM – GIAC Security Operations Manager
GSSP – GIAC Secure Software Programmer
GSTRT – GIAC Strategic Planning, Policy, and Leadership
GWAPT – GIAC Web Application Penetration Tester
GWEB – GIAC Certified Web Application Defender
GXPN – GIAC Exploit Researcher and Advanced Penetration Tester
LPT – EC Council Licensed Penetration Tester
OSCE3 – Offensive Security Certified Expert 3
OSCP – Offensive Security Certified Professional
OSED – Offensive Security Exploit Developer
OSEE – Offensive Security Exploitation Expert
OSEP – Offensive Security Experienced Penetration Tester
OSMR – Offensive Security macOS Researcher
OSWA – Offensive Security Web Assessor
OSWE – Offensive Security Web Expert
OSWP – Offensive Security Wireless Professional
PenTest+ – CompTIA PenTest+
Security+ – CompTIA Security+
SSCP – Systems Security Certified Practitioner

UZASADNIENIE

Projekt stanowi realizację upoważnienia ustawowego do wydania aktu wykonawczego przez Radę Ministrów, na podstawie art. 8 ust. 1 ustawy z dnia 2 grudnia 2021 r. o szczególnych zasadach wynagradzania osób realizujących zadania z zakresu cyberbezpieczeństwa (Dz. U. poz. 2333), zwanej dalej „ustawą”.

Rozporządzenie określa:

1) szczegółowe zadania z zakresu cyberbezpieczeństwa i podział ich na grupy;
2) doświadczenie zawodowe lub wymóg posiadania specjalistycznej wiedzy z zakresu cyberbezpieczeństwa wymagane do realizacji zadań z poszczególnych grup;
3) przedziały kwotowe wysokości świadczenia teleinformatycznego w związku z podziałem zadań z zakresu cyberbezpieczeństwa na grupy, o których mowa w pkt 1.

Wzrastająca liczba incydentów cyberbezpieczeństwa oraz pojawiające się nowe zagrożenia, jak również coraz większa dostępność usług publicznych online, powodują, że instytucje publiczne odpowiedzialne za cyberbezpieczeństwo państwa potrzebują dysponować wysoko wykwalifikowaną kadrą. Rynek specjalistów z zakresu cyberbezpieczeństwa jest jednak rynkiem bardzo konkurencyjnym. Wynagrodzenia oferowane w sektorze prywatnym znacznie przewyższają wynagrodzenia oferowane przez instytucje publiczne, które są ograniczane określonymi widełkami płacowymi. Szczególnie negatywnym zjawiskiem jest odpływ kadr z sektora publicznego na rzecz podjęcia pracy na rynku prywatnym. Niezbędne jest zatem wprowadzenie odpowiednich rozwiązań, które pozwolą na utrzymanie specjalistów z zakresu cyberbezpieczeństwa w sektorze publicznym, w szczególności poprzez polepszenie ich sytuacji ekonomicznej.

Wprowadzane świadczenie teleinformatyczne, finansowane z Funduszu Cyberbezpieczeństwa, zapewni konkurencyjne wynagrodzenia dla specjalistów zajmujących się cyberbezpieczeństwem w sektorze publicznym. Rozwiązanie to wpisuje się w cele określone w Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024, zgodnie z którą podjąć należy działania zwiększające zarobki pracowników administracji publicznej, zajmujących się cyberbezpieczeństwem, do poziomu, jaki mogliby uzyskać zatrudniając się w sektorze prywatnym[1)].

[1)] Pkt 8.1 załącznika do uchwały nr 125 Rady Ministrów z dnia 22 października 2019 r. w sprawie Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024 (M.P. poz. 1037).

W tabeli zawartej w załączniku do rozporządzenia, określone zostały zadania, za których wykonywanie będzie mogło zostać przyznane świadczenie teleinformatyczne, takie jak m.in.: analiza szkodliwego oprogramowania, czy analiza powłamaniowa (*forensic*), wykrywanie zagrożeń lub incydentów (*cyber threat intelligence*), a także tworzenie rekomendacji technicznych oraz ogólnych z obszaru cyberbezpieczeństwa, czy prowadzenie nadzoru nad podmiotami krajowego systemu cyberbezpieczeństwa. Do tych zadań zostały dodane zadania techniczne związane z zapewnianiem cyberbezpieczeństwa w samych jednostkach administracji, w szczególności obsługa incydentów, a także inne zadania pomocnicze, które realizują ten cel.

Zadania zostały ułożone w grupy według maksymalnych kwot, jakie będą mogły zostać przyznane za ich realizację. Wykaz zadań zawartych w rozporządzeniu ma charakter zamknięty. Katalog ten powinien zostać w przyszłości poddawany stosownym przeglądom.

Do grup o najwyższych kwotach zostały przyporządkowane najważniejsze zadania z zakresu cyberbezpieczeństwa, takie jak: ocena bezpieczeństwa systemów IT – w tym testy penetracyjne i audyty bezpieczeństwa, analizowanie szkodliwego oprogramowania, czy też kierowanie jednostką organizacyjną przeznaczoną do realizacji zadań z zakresu cyberbezpieczeństwa. Są to zadania kluczowe z punktu widzenia zapewnienia cyberbezpieczeństwa we wszystkich kluczowych podmiotach. Realizacja tych zadań wymaga również posiadania szczególnej, specjalistycznej wiedzy.

Do kolejnych grup przyporządkowano istotne zadania wymagające wiedzy oraz umiejętności technicznych i analitycznych, takie jak: przygotowywanie rekomendacji, standardów i dobrych praktyk w zakresie cyberbezpieczeństwa, w szczególności podnoszących poziom bezpieczeństwa systemów IT będących w dyspozycji podmiotów krajowego systemu cyberbezpieczeństwa, czy też utrzymanie i rozwój istotnych systemów IT w ramach organizacji.

Do ostatniej grupy zaliczono zadania wspierające oraz administracyjne, takie jak m.in.: prowadzenie postepowań wobec operatorów usług kluczowych, sprawowanie nadzoru nad podmiotami krajowego systemu cyberbezpieczeństwa oraz prowadzenie akcji podnoszących świadomość w obszarze cyberbezpieczeństwa. Tego typu zadania są również niezwykle istotne z punktu widzenia sprawnego działania całego systemu cyberbezpieczeństwa w Polsce.

W zależności od stopnia skomplikowania danego zadania oraz szczególnych kompetencji, jakie są wymagane do jego wykonywania, kwoty świadczenia zostały zróżnicowane

w zależności od posiadanego doświadczenia, tj. podzielono je na 2 lub 3 przedziały. Większa liczba przedziałów została wyodrębniona w przypadku szczególnie istotnych zadań oraz takich, gdzie korzystne będą dodatkowe zachęty do zdobywania doświadczenia w danej, szczególnie wysokospecjalistycznej dziedzinie.

Progi finansowe zostały przygotowane w taki sposób, by zapewnić najwyższe wartości świadczeń dla wąskiej grupy specjalistów zajmujących się technicznymi aspektami cyberbezpieczeństwa. Tych specjalistów jest niewielu i są oni szczególnie poszukiwani na rynku pracy. Ustalane rozporządzeniem przedziały i wartości świadczenia teleinformatycznego znajdują uzasadnienie w tej sytuacji rynkowej.

Przedziały kwotowe wysokości świadczenia teleinformatycznego mają zapewnić wynagrodzenia konkurencyjne dla osób realizujących zadania w obszarze cyberbezpieczeństwa na rynku prywatnym. Uwzględniono również konieczność zapewnienia zasobów kadrowych odpowiednich do efektywnej i skutecznej realizacji zadań, a zatem posiadających specjalistyczną wiedzę dotyczącą metod i narzędzi wykorzystywanych do zapewnienia odporności systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy. Osoby wykonujące zadania w ramach instytucji odpowiedzialnych w szczególny sposób za bezpieczeństwo państwa, otrzymają świadczenia adekwatne do ich roli.

Zgodnie z art. 8 ust. 6 ustawy kierownik podmiotu może odstąpić od przeprowadzenia sprawdzianu wiedzy w przypadku przedłożenia przez osobę realizującą albo mającą realizować zadania z zakresu cyberbezpieczeństwa, aktualnego dokumentu potwierdzającego posiadanie specjalistycznej wiedzy z zakresu cyberbezpieczeństwa w zakresie zgodnym z zadaniami na stanowisku. W związku z tym w załączniku wskazano dokumenty na podstawie, których weryfikowane będzie specjalistyczna wiedza niezbędna do wykonywania poszczególnych zadań. Wskazane zostały międzynarodowe certyfikaty oraz dokumenty odwołujące się wprost do norm z dziedziny bezpieczeństwa informacji. Ich wskazanie zapewni, że świadczenie otrzymają wykwalifikowani specjaliści, kluczowi dla bezpieczeństwa całego systemu cyberbezpieczeństwa.

Rozporządzenie wejdzie w życie po upływie 5 dni od dnia ogłoszenia. Z uwagi na przyjęte w projekcie rozwiązania prawne proponowany termin wejścia w życie niniejszego rozporządzenia nie narusza zasady demokratycznego państwa prawnego.

Ponadto, należy podkreślić, że rozporządzenie jest niezbędne dla prawidłowego funkcjonowania ustawy, która wejdzie w życie w dniu 1 stycznia 2022 r.

Ze względu na powyższe projekt jest procedowany w trybie odrębnym, zgodnie z § 98 i n. uchwały nr 190 Rady Ministrów z dnia 29 października 2013 r. – Regulamin pracy Rady Ministrów.

Projektowane przepisy zostały przeanalizowane pod kątem wpływu na małe i średnie przedsiębiorstwa. Przyjęte w projekcie rozwiązania nie będą miały wpływu na działalność mikroprzedsiębiorców, małych i średnich przedsiębiorców, stosownie do przepisu art. 66 ust. 1 pkt 2 ustawy z dnia 6 marca 2018 r. – Prawo przedsiębiorców (Dz. U. z 2021 r. poz. 162).

Projektowane rozporządzenie nie będzie mieć wpływu na sytuację ekonomiczną i społeczną rodziny, osób niepełnosprawnych oraz osób starszych.

Projektowana regulacja nie zawiera przepisów technicznych w rozumieniu rozporządzenia Rady Ministrów z dnia 23 grudnia 2002 r. w sprawie sposobu funkcjonowania krajowego systemu notyfikacji norm i aktów prawnych (Dz. U. poz. 2039 oraz z 2004 r. poz. 597) i nie podlega notyfikacji Komisji Europejskiej.

Projektowana regulacja nie wymaga notyfikacji Komisji Europejskiej w trybie ustawy z dnia 30 kwietnia 2004 r. o postępowaniu w sprawach dotyczących pomocy publicznej (Dz. U. z 2021 r. poz. 743).

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

Stosownie do postanowień art. 5 ustawy z dnia 7 lipca 2005 r. o działalności lobbingowej w procesie stanowienia prawa (Dz. U. z 2017 r. poz. 248), projekt rozporządzenia został udostępniony w Biuletynie Informacji Publicznej.

W projekcie nie zawarto przepisów o charakterze przejściowym ze względu na brak stosunków prawnych powstałych przed datą wejścia w życie tego rozporządzenia, na które projektowane rozporządzenie miałoby wpływ.

OCENA SKUTKÓW REGULACJI

Nazwa projektu Rozporządzenie Rady Ministrów w sprawie wysokości świadczenia teleinformatycznego osób realizujących zadania z zakresu cyberbezpieczeństwa. **Ministerstwo wiodące i ministerstwa współpracujące** Kancelaria Prezesa Rady Ministrów **Osoba odpowiedzialna za projekt w randze Ministra, Sekretarza Stanu lub Podsekretarza Stanu** Janusz Cieszyński, Sekretarz Stanu w KPRM **Kontakt do opiekuna merytorycznego projektu** Łukasz Wojewoda, Dyrektor Departamentu Cyberbezpieczeństwa, e-mail: sekretariat.dc@mc.gov.pl Marcin Wysocki, Zastępca Dyrektora Departamentu Cyberbezpieczeństwa, e-mail: sekretariat.dc@mc.gov.pl	**Data sporządzenia** 23 grudnia 2021 r. **Źródło:** Upoważnienie ustawowe z art. 8 ust. 1 ustawy z dnia 2 grudnia 2021 r. o szczególnych zasadach wynagradzania osób realizujących zadania z zakresu cyberbezpieczeństwa. **Nr w wykazie prac: RD472**

OCENA SKUTKÓW REGULACJI

1. Jaki problem jest rozwiązywany?

Projekt rozporządzenia stanowi wykonanie upoważnienia ustawowego zawartego w art. 8 ust. 1 ustawy z dnia 2 grudnia 2021 r. o szczególnych zasadach wynagradzania osób realizujących zadania z zakresu cyberbezpieczeństwa (zwana dalej „ustawą").

W rozporządzeniu ustalane są szczegółowe zadania z zakresu cyberbezpieczeństwa w podziale na grupy, doświadczenie zawodowe lub wymóg posiadania specjalistycznej wiedzy wymagane do realizacji zadań z poszczególnych grup oraz przedziały kwotowe wysokości świadczenia teleinformatycznego.

Projektowana regulacja umożliwi wyrównanie wynagrodzeń ww. osób do wynagrodzeń jakie mogłyby otrzymać na rynku, tym samym ograniczając odpływ specjalistów z administracji publicznej. W konsekwencji projektowane rozwiązanie pozytywnie wpłynie na poziom cyberbezpieczeństwa w Rzeczypospolitej Polskiej.

Rozwiązanie to wpisuje się w cele określone w Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024, zgodnie z którą podejmowane mają być działania zwiększające zarobki pracowników administracji publicznej, zajmujących się cyberbezpieczeństwem, do poziomu, jaki mogliby uzyskać, zatrudniając się w sektorze prywatnym.

2. Rekomendowane rozwiązanie, w tym planowane narzędzia interwencji, i oczekiwany efekt

Rozporządzenie określa:

1) szczegółowe zadania z zakresu cyberbezpieczeństwa i podział ich na grupy;

2) doświadczenie zawodowe lub wymóg posiadania specjalistycznej wiedzy z zakresu cyberbezpieczeństwa wymagane do realizacji zadań z poszczególnych grup;

3) przedziały kwotowe wysokości świadczenia teleinformatycznego w związku z podziałem zadań z zakresu cyberbezpieczeństwa na grupy, o których mowa w pkt 1.

W tabeli zawartej w załączniku do rozporządzenia określone zostały zadania, za których wykonywanie będzie mogło zostać przyznane świadczenie teleinformatyczne, takie jak m.in. analiza szkodliwego oprogramowania, czy analiza powłamaniową (forensic), wykrywanie zagrożeń lub incydentów (cyber threat intelligence), a także tworzenie rekomendacji technicznych oraz ogólnych z obszaru cyberbezpieczeństwa, czy prowadzenie nadzoru nad podmiotami krajowego systemu cyberbezpieczeństwa. Do tych zadań zostały dodane zadania techniczne związane z zapewnianiem cyberbezpieczeństwa w samych jednostkach administracji, w szczególności obsługa incydentów, a także inne zadania pomocnicze, które realizują ten cel.
Ustalane rozporządzeniem maksymalne wartości świadczenia teleinformatycznego znajdują uzasadnienie w sytuacji rynkowej. Jednocześnie wzmocnienia wymagają także zasoby kadrowe odpowiedzialne za funkcjonowanie pod względem prawnym i organizacyjnym krajowego systemu cyberbezpieczeństwa.
Wymóg doświadczenia zawodowego został zróżnicowany w zależności od zadania. W przypadku zadań wymagających największej wiedzy i kwalifikacji, odnosząc się do doświadczenia dodatkowo oparto się na rozwiązaniach rynkowych stosowanych w branży IT.
Tak przygotowane rozporządzenie będzie stanowiło podstawę do przyznawania świadczeń teleinformatycznych już od 2022 r. Przygotowane rozwiązania zapewniają, że nowe środki wzmocnią instytucje odpowiedzialne za cyberbezpieczeństwo państwa i pozwolą im utrzymać obecnych pracowników jak i zatrudnić nowych ekspertów w dziedzinie cyberbezpieczeństwa.

3. Jak problem został rozwiązany w innych krajach, w szczególności krajach członkowskich OECD/UE?

Brak danych.

4. Podmioty, na które oddziałuje projekt

Grupa	Wielkość	Źródło danych	Oddziaływanie
osoby, które będą mogły otrzymać świadczenie teleinformatyczne	ok. 1000	Szacunki KPRM	Pozytywne, osoby te otrzymają świadczenie teleinformatyczne
Minister właściwy do spraw informatyzacji	1	Informacja ogólnodostępna	Minister właściwy do spraw informatyzacji będzie dysponentem Funduszu Cyberbezpieczeństwa.

5. Informacje na temat zakresu, czasu trwania i podsumowanie wyników konsultacji

Ze względu na to, że rozporządzenie jest niezbędne do wykonania upoważnienia określonego w art. 8 ust. 1 ustawy z dnia 2 grudnia 2021 r. o szczególnych zasadach wynagradzania osób realizujących zadania z zakresu cyberbezpieczeństwa, która wchodzi w życie w dniu 1 stycznia 2022 r. projekt jest procedowany w trybie odrębnym, zgodnie z § 98 i n. uchwały nr 190 Rady Ministrów z dnia 29 października 2013 r. – Regulamin pracy Rady Ministrów.
W związku z powyższym, projekt nie został skierowany do uzgodnień, opiniowania i konsultacji publicznych, a jedynie został przekazany bezpośrednio do rozpatrzenia przez Radę Ministrów.

6. Wpływ na sektor finansów publicznych

	Skutki w okresie 10 lat od wejścia w życie zmian [mln zł]

(ceny stałe z 2021 r.)	0	1	2	3	4	5	6	7	8	9	10	*Łącznie (0-10)*
Dochody ogółem	0	0	0	0	0	0	0	0	0	0	0	0
budżet państwa	0	0	0	0	0	0	0	0	0	0	0	0
JST	0	0	0	0	0	0	0	0	0	0	0	0
pozostałe jednostki (oddzielnie)	0	0	0	0	0	0	0	0	0	0	0	0
Wydatki ogółem	0	0	0	0	0	0	0	0	0	0	0	0
budżet państwa	0	0	0	0	0	0	0	0	0	0	0	0
JST	0	0	0	0	0	0	0	0	0	0	0	0
pozostałe jednostki (oddzielnie)	0	0	0	0	0	0	0	0	0	0	0	0
Saldo ogółem	0	0	0	0	0	0	0	0	0	0	0	0
budżet państwa	0	0	0	0	0	0	0	0	0	0	0	0
JST	0	0	0	0	0	0	0	0	0	0	0	0
pozostałe jednostki (oddzielnie)	0	0	0	0	0	0	0	0	0	0	0	0
Źródła finansowania	Fundusz Cyberbezpieczeństwa utworzony na mocy ustawy z dnia 2 grudnia 2021 r. o szczególnych zasadach wynagradzania osób realizujących zadania z zakresu cyberbezpieczeństwa											
Dodatkowe informacje, w tym wskazanie źródeł danych i przyjętych do obliczeń założeń	Wejście w życie projektu rozporządzenia nie spowoduje dodatkowych obciążeń finansowych dla sektora finansów publicznych, w tym dla budżetu państwa i budżetów jednostek samorządu terytorialnego.											

7. Wpływ na konkurencyjność gospodarki i przedsiębiorczość, w tym funkcjonowanie przedsiębiorców oraz na rodzinę, obywateli i gospodarstwa domowe

Skutki								
Czas w latach od wejścia w życie zmian		0	1	2	3	5	10	*Łącznie (0-10)*
W ujęciu pieniężnym (w mln zł, ceny stałe z 2021 r.)	duże przedsiębiorstwa	-	-	-	-	-	-	-
	sektor mikro-, małych i średnich przedsiębiorstw	-	-	-	-	-	-	-
	rodzina, obywatele oraz gospodarstwa domowe	-	-	-	-	-	-	-
	(dodaj/usuń)	-	-	-	-	-	-	-
W ujęciu niepieniężnym	duże przedsiębiorstwa	Projekt nie ma wpływu na duże przedsiębiorstwa.						
	sektor mikro-, małych i	Projekt nie ma wpływu na sektor mikro-, małych i średnich przedsiębiorstw.						

	średnich przedsiębiorstw	
	rodzina, obywatele oraz gospodarstwa domowe	Projekt będzie miał pozytywny wpływ na cyberbezpieczeństwo Państwa, co pozwoli na zapewnienie bezpiecznych cyfrowych usług publicznych dla obywateli.
	(dodaj/usuń)	
Niemierzalne	(dodaj/usuń)	
	(dodaj/usuń)	
Dodatkowe informacje, w tym wskazanie źródeł danych i przyjętych do obliczeń założeń		

8. Zmiana obciążeń regulacyjnych (w tym obowiązków informacyjnych) wynikających z projektu

☐ nie dotyczy

Wprowadzane są obciążenia poza bezwzględnie wymaganymi przez UE (szczegóły w odwróconej tabeli zgodności).	☐ tak ☐ nie ☒ nie dotyczy
☐ zmniejszenie liczby dokumentów ☐ zmniejszenie liczby procedur ☐ skrócenie czasu na załatwienie sprawy ☐ inne:	☐ zwiększenie liczby dokumentów ☒ zwiększenie liczby procedur ☐ wydłużenie czasu na załatwienie sprawy ☐ inne:
Wprowadzane obciążenia są przystosowane do ich elektronizacji.	☒ tak ☐ nie ☐ nie dotyczy
Komentarz:	

9. Wpływ na rynek pracy

Projekt pozytywnie wpłynie na podmioty publiczne zajmujące się cyberbezpieczeństwem Państwa, które będą mogły zaoferować specjalistom z zakresu cyberbezpieczeństwa konkurencyjne warunki finansowe, w stosunku do warunków oferowanych przez sektor prywatny.

10. Wpływ na pozostałe obszary

☐ środowisko naturalne ☐ sytuacja i rozwój regionalny ☐ sądy powszechne, administracyjne lub wojskowe	☐ demografia ☐ mienie państwowe ☐ inne:	☒ informatyzacja ☐ zdrowie
Omówienie wpływu	Wprowadzenie rozporządzenia podniesie poziom cyberbezpieczeństwa Państwa poprzez odpowiednie wynagrodzenie kadry specjalistów oraz zwiększenie możliwości zatrudnienia przez podmioty określone w art. 5 ustawy, wysoko wykwalifikowanej kadry z obszaru cyberbezpieczeństwa.	

11. Planowane wykonanie przepisów aktu prawnego

Rozporządzenie stanowić będzie podstawę do sporządzenia i złożenia przez kierownika podmiotu, o którym mowa w art. 5 ustawy wniosku, celem uzyskania środków z Funduszu Cyberbezpieczeństwa na sfinansowanie świadczenia teleinformatycznego dla pracowników tego podmiotu. Pierwsze wnioski będą mogły być złożone do 21 stycznia 2022 r.
12. W jaki sposób i kiedy nastąpi ewaluacja efektów projektu oraz jakie mierniki zostaną zastosowane?
W ciągu roku od dnia wejścia w życie rozporządzenia zostanie przeprowadzona analiza mająca na celu zweryfikowanie wykazu zadań ujętych w załączniku do rozporządzenia.
13. Załączniki (istotne dokumenty źródłowe, badania, analizy itp.)