

Warszawa, dnia 20 stycznia 2022 r.

Poz. 131

**ROZPORZĄDZENIE  
RADY MINISTRÓW**

z dnia 19 stycznia 2022 r.

**w sprawie wysokości świadczenia teleinformatycznego dla 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 dla osób realizujących zadania z zakresu cyberbezpieczeństwa, stanowiącą załącznik do rozporządzenia.

**§ 3.** Rozporządzenie wchodzi w życie z dniem ogłoszenia.

Prezes Rady Ministrów: *M. Morawiecki*

Załącznik do rozporządzenia Rady Ministrów  
z dnia 19 stycznia 2022 r. (poz. 131)

TABELA SZCZEGÓŁOWYCH ZADAŃ Z ZAKRESU CYBERBEZPIECZEŃSTWA  
ORAZ DOŚWIADCZENIA ZAWODOWEGO LUB POSIADANIA SPECJALISTYCZNEJ WIEDZY  
W ZAKRESIE CYBERBEZPIECZEŃSTWA, A TAKŻE PRZEDZIAŁY KWOTOWE WYSOKOŚCI ŚWIADCZENIA  
TELEINFORMATYCZNEGO DLA OSÓB REALIZUJĄCYCH ZADANIA Z ZAKRESU CYBERBEZPIECZEŃSTWA

Nr grupy	Doświadczenie zawodowe w realizacji zadań w zakresie cyberbezpieczeństwa	Przedziały kwotowe wysokości świadczenia teleinformatycznego w złotych		Szczegółowe zadania z zakresu cyberbezpieczeństwa	Wymóg posiadania specjalistycznej wiedzy w zakresie cyberbezpieczeństwa, o której mowa co najmniej w jednym z poniższych dokumentów
1	do 3 lat	2000	12 000	<ol style="list-style-type: none"> <li>Aktywne poszukiwanie zagrożeń cyberbezpieczeństwa (Cyber Threat Intelligence i Threat Hunting)</li> <li>Analiza złośliwego oprogramowania</li> <li>Badanie bezpieczeństwa, podatności i testowanie sprzętu lub oprogramowania</li> <li>Ocena bezpieczeństwa systemów informacyjnych, w tym testy penetracyjne i audyty bezpieczeństwa</li> <li>Prowadzenie specjalistycznych analiz cyberbezpieczeństwa i wykrywanie nowych podatności</li> <li>Rozwijanie specjalistycznych narzędzi technicznych wspomagających realizację zadań z zakresu cyberbezpieczeństwa</li> </ol>	<p>CASP+, CCFE, CEH, CEH Master, Certyfikat audytora wiodącego systemu zarządzania bezpieczeństwem informacji według normy PN-EN ISO/IEC 27001, CPENT, CSSLP, CHFI, CMFE, CPT, eCDFP, eCMAP, CISSP, COBIT Foundation, GASF, GAWN, GCCC, GCDA, GCFA, GCPN, GCTI, GNFA, GPEN, GREM, GSNA, GMOB, GSSP, GWAPT, GWEB, GXPN, ITIL Foundation, LPT, OSCE3, OSCP, OSED, OSEP, OSEE, OSMR, OSWA, OSWE, OSWP, PenTest+ lub w innym równoważnym dokumencie,</p> <p>lub w dokumencie potwierdzającym zajęcie jednego z trzech pierwszych miejsc w zawodach, treningach, turniejach lub ćwiczeniach z zakresu cyberbezpieczeństwa,</p>
	od 3 do 5 lat		18 000		
	powyżej 5 lat		30 000		

					<p>w szczególności w:</p> <ol style="list-style-type: none"> <li>1. Core NetWars Tournament<sup>1)</sup></li> <li>2. Cyber Defense NetWars<sup>2)</sup></li> <li>3. DFIR NetWars Tournament<sup>3)</sup></li> <li>4. Grid NetWars Tournament<sup>4)</sup></li> <li>5. ICS NetWars Tournament<sup>5)</sup></li> </ol> <p>lub w dokumencie potwierdzającym udział w zespole, który w przeciągu ostatnich pięciu lat zajął przynajmniej raz w klasyfikacji polskich zespołów piąte lub lepsze miejsce w światowym rankingu CTFtime</p>
2	do 3 lat	2000	12 000	<ol style="list-style-type: none"> <li>1. Kierowanie jednostką lub komórką organizacyjną przeznaczoną do realizacji zadań z zakresu cyberbezpieczeństwa</li> <li>2. Prowadzenie działań prewencyjnych zwiększających cyberbezpieczeństwo</li> <li>3. Prowadzenie zaawansowanych działań z zakresu aktywnej obrony systemów informacyjnych</li> <li>4. Zaawansowana obsługa incydentów</li> </ol>	<p>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 innym równoważnym dokumencie,</p> <p>lub w dokumencie potwierdzającym zajęcie jednego z trzech pierwszych miejsc w zawodach, treningach, turniejach lub ćwiczeniach z zakresu cyberbezpieczeństwa,</p> <p>w szczególności w:</p> <ol style="list-style-type: none"> <li>1. Core NetWars Tournament</li> <li>2. Cyber Defense NetWars</li> <li>3. DFIR NetWars Tournament</li> <li>4. Grid NetWars Tournament</li> <li>5. ICS NetWars Tournament</li> </ol>
	od 3 do 5 lat		18 000		
	powyżej 5 lat		25 000		

<sup>1)</sup> <https://www.sans.org/cyber-ranges/netwars-tournaments/core/>

<sup>2)</sup> <https://www.sans.org/cyber-ranges/netwars-tournaments/cyber-defense/>

<sup>3)</sup> <https://www.sans.org/cyber-ranges/netwars-tournaments/digital-forensics-incident-response/>

<sup>4)</sup> <https://www.sans.org/cyber-ranges/netwars-tournaments/power-grid/>

<sup>5)</sup> <https://www.sans.org/cyber-ranges/netwars-tournaments/industrial-control-system-security/>

3	do 3 lat	2000	8000	<ol style="list-style-type: none"> <li>1. Analiza powłamaniowa</li> <li>2. Badanie i ocena bezpieczeństwa rozwiązań ICT</li> <li>3. Projektowanie, budowa i utrzymanie systemów monitorowania i detekcji incydentów oraz wsparcia funkcjonowania operacyjnego centrum bezpieczeństwa (SOC)/Zespołu Reagowania na Incydenty Bezpieczeństwa Komputerowego (CSIRT)</li> <li>4. Korelacja danych, prowadzenie analiz lub tworzenie map sytuacyjnych</li> <li>5. Monitorowanie zagrożeń cyberbezpieczeństwa i incydentów na poziomie krajowym</li> <li>6. Prowadzenie analiz incydentów poważnych, powiązań między incydentami oraz opracowywanie wniosków</li> <li>7. Przyjmowanie zgłoszeń i obsługa incydentów poważnych</li> <li>8. Reagowanie na incydenty oraz ich klasyfikacja</li> </ol>	<p>BTL1, BTL2, CAP, CASP+, CAWFE, CEH, CEH Master, CISM, CCFE, CDRP, CFSR, CISSP, CHFI, COBIT Foundation, CPENT, CSSLP, CNFE, CySA+, eCDFP, eCMAP, GCCC, GCDA, GCFA, GCFE, GCIH, GCSA, GISP, GMON, GNFA, GASF, GSE, GSLC, GSOC, GSOM, GWEB, OSCP, OSEE, OSEP, PenTest+, Security+, SSCP lub w innym równoważnym dokumencie,</p> <p>lub w dokumencie potwierdzającym zajęcie jednego z trzech pierwszych miejsc w zawodach, treningach, turniejach lub ćwiczeniach z zakresu cyberbezpieczeństwa, w szczególności w:</p> <ol style="list-style-type: none"> <li>1. Core NetWars Tournament</li> <li>2. Cyber Defense NetWars</li> <li>3. DFIR NetWars Tournament</li> <li>4. Grid NetWars Tournament</li> <li>5. ICS NetWars Tournament</li> </ol>
	od 3 do 5 lat		12 000		
	powyżej 5 lat		20 000		
4	do 3 lat	2000	6000	<ol style="list-style-type: none"> <li>1. Analiza i zarządzanie w zakresie reagowania na wykryte podatności sprzętu i oprogramowania</li> <li>2. Koordynacja obsługi zgłoszonych incydentów</li> <li>3. Obsługa zgłoszeń i analiza treści przypadków dystrybucji, rozpowszechniania lub przesyłania pornografii dziecięcej za pośrednictwem technologii informacyjno-komunikacyjnych</li> <li>4. Specjalistyczne zadania realizowane w ramach SOC lub Centrum Zarządzania Siecią (NOC) obejmujące: monitoring</li> </ol>	<p>BTL1, BTL2, CASP+, CEH, CEH Master, CISSP, COBIT Foundation, CPENT, CySA+, GCIH, GCDA, GDAT, GISP, GMON, GSLC, GSOC, GSTRT, ITIL Foundation, OSCP, Security+, SSCP lub w innym równoważnym dokumencie,</p> <p>lub w dokumencie potwierdzającym zajęcie jednego z trzech pierwszych miejsc w zawodach, treningach, turniejach lub ćwiczeniach z zakresu cyberbezpieczeństwa, w szczególności w:</p> <ol style="list-style-type: none"> <li>1. Core NetWars Tournament</li> </ol>
	od 3 do 5 lat		9000		
	powyżej 5 lat		15 000		

				bezpieczeństwa (analiza i korelacja logów), identyfikację i wstępną obsługę incydentów	<ol style="list-style-type: none"> <li>2. Cyber Defense NetWars</li> <li>3. DFIR NetWars Tournament</li> <li>4. Grid NetWars Tournament</li> <li>5. ICS NetWars Tournament</li> </ol>
5	do 3 lat	2000	5500	<ol style="list-style-type: none"> <li>1. Szacowanie ryzyka w obszarze cyberbezpieczeństwa</li> <li>2. Opracowywanie i wdrażanie planów ciągłości działania i odbudowy oraz systemu zarządzania bezpieczeństwem informacji</li> <li>3. Nadzór nad procesem szacowania ryzyka w obszarze cyberbezpieczeństwa</li> </ol>	<p>Certified Reliability Professional, Certyfikat audytora wiodącego systemu zarządzania bezpieczeństwem informacji według normy PN-EN ISO/IEC 27001, Certyfikat audytora wiodącego systemu zarządzania ciągłością działania PN-EN ISO 22301, Certyfikaty uprawniające do posiadania tytułu ISA/IEC 62443 Cybersecurity Expert, CGEIT, CIA, CISA, CISM, CISSP, CRISC, SSCP, CBCI, CBCP lub w innym równoważnym dokumencie</p>
	od 3 do 5 lat		8500		
	powyżej 5 lat		13 500		
6	do 3 lat	2000	5000	Przygotowywanie rekomendacji, standardów i dobrych praktyk w zakresie cyberbezpieczeństwa, w szczególności podnoszących poziom bezpieczeństwa systemów informacyjnych będących w dyspozycji podmiotów krajowego systemu cyberbezpieczeństwa	<p>CAP, CASP+, CEH, CISA, CISSP, GISP, GSE, GSLC, GSNA, SSCP lub w innym równoważnym dokumencie, lub w dokumencie potwierdzającym zajęcie jednego z trzech pierwszych miejsc w zawodach, treningach, turniejach lub ćwiczeniach z zakresu cyberbezpieczeństwa, w szczególności w:</p> <ol style="list-style-type: none"> <li>1. Core NetWars Tournament</li> <li>2. Cyber Defense NetWars</li> <li>3. DFIR NetWars Tournament</li> </ol>
	od 3 do 5 lat		8000		
	powyżej 5 lat		12 000		

					4. Grid NetWars Tournament 5. ICS NetWars Tournament
7	do 3 lat	2000	4500	<ol style="list-style-type: none"> <li>1. Bieżące utrzymanie i rozwój własnych, istotnych systemów informacyjnych</li> <li>2. Poszukiwanie znanych podatności sprzętu i oprogramowania w nadzorowanych systemach teleinformatycznych</li> <li>3. Wstępna obsługa incydentów</li> <li>4. Zabezpieczenie śladów cyfrowych</li> <li>5. Rozpoznawanie zagrożeń cyberbezpieczeństwa</li> </ol>	<p>BTL1, CASP+, CEH, CEH Master, CISA, CPENT, CSSLP, CySA+, GBFA, GCIH, GMON, GOSI, ITIL Foundation, ITIL Managing Professional, ITIL Master, OSCP, OSEE, OSEP, PenTest+, Security+, SSCP lub w innym równoważnym dokumencie,</p> <p>lub w dokumencie potwierdzającym zajęcie jednego z trzech pierwszych miejsc w zawodach, treningach, turniejach lub ćwiczeniach z zakresu cyberbezpieczeństwa, w szczególności w:</p> <ol style="list-style-type: none"> <li>1. Core NetWars Tournament</li> <li>2. Cyber Defense NetWars</li> <li>3. DFIR NetWars Tournament</li> <li>4. Grid NetWars Tournament</li> <li>5. ICS NetWars Tournament</li> </ol>
	od 3 do 5 lat		6000		
	powyżej 5 lat		10 500		
8	do 3 lat	2000	6000	<ol style="list-style-type: none"> <li>1. Identyfikacja oraz prowadzenie postępowań wobec operatorów usług kluczowych</li> <li>2. Nadzór nad podmiotami krajowego systemu cyberbezpieczeństwa</li> <li>3. Nadzór nad podmiotami świadczącymi usługi z zakresu cyberbezpieczeństwa</li> <li>4. Prowadzenie akcji podnoszących świadomość w obszarze cyberbezpieczeństwa, w szczególności organizacja ćwiczeń i szkoleń</li> <li>5. Prowadzenie analiz w zakresie funkcjonowania krajowego systemu</li> </ol>	<p>CASP+, CEH, CGAP, CIA, CISA, CISM, CISSP, GISP, GSLC, Security+ lub w innym równoważnym dokumencie</p>
	powyżej 3 lat		8000		

				<p>cyberbezpieczeństwa, w tym w zakresie rozwiązań prawnych, organizacyjnych, standardów oraz certyfikacji w obszarze cyberbezpieczeństwa wraz z przygotowaniem projektów aktów normatywnych</p> <p>6. Prowadzenie analiz w zakresie spełniania przez podmioty z sektora lub podsektora warunków kwalifikujących podmiot jako operatora usługi kluczowej</p> <p>7. Prowadzenie kontroli w podmiotach krajowego systemu cyberbezpieczeństwa, w tym w podmiotach świadczących usługi z zakresu cyberbezpieczeństwa</p> <p>8. Współpraca krajowa lub międzynarodowa w obszarze cyberbezpieczeństwa</p>	
--	--	--	--	---	--

**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

CBCI – Certificate of Business Continuity Institute

CBCP – Certified Business Continuity Professional

CCFE – Certified Computer Forensics Examiner

CDRP – Certified Data Recovery Professional

CEH – Certified Ethical Hacker

CEH Master – Certified Ethical Hacker Master

Certified Reliability Professional

Certyfikat audytora wiodącego systemu zarządzania bezpieczeństwem informacji według normy PN-EN ISO/IEC 27001

Certyfikat audytora wiodącego systemu zarządzania ciągłością działania PN-EN ISO 22301

Certyfikaty uprawniające do posiadania tytułu ISA/IEC 62443 Cybersecurity Expert

CFSR – Certified Forensic Security Responder

CGAP – Certified Government Auditing Professional

CGEIT – ISACA's Certified in the Governance of Enterprise IT

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  
COBIT Foundation  
CPENT – Certified Penetration Testing Professional  
CPT – Certified Penetration Tester  
CRISC – ISACA’s Certified in Risk and Information Systems Control  
CSSLP – Certified Secure Software Lifecycle Professional  
CySA+ – CompTIA CySA+  
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  
ITIL Foundation  
ITIL Managing Professional  
ITIL Master  
LPT – EC Council Licensed Penetration Tester  
OSCE3 – Offensive Security Certified Expert 3  
OSCP – Offensive Security Certified Professional



OSD – 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