OLIMPIADA WIEDZY O BEZPIECZEŃSTWIE I OBRONNOŚCI

.....
(imię i nazwisko)

.....
(liczba punktów)

Olimpiada Wiedzy o Bezpieczeństwie i Obronności

X edycja

Etap okręgowy

12.12.2025 r. Czas pracy: 60 minut

Instrukcja dla uczestnika

1. Sprawdź, czy test zawiera 8 stron (zadania 1-40). Ewentualne braki zgłoś Przewodniczącemu Zespołu Nadzorującego. Podpisz arkusz w wyznaczonym miejscu.
2. Pamiętaj, że rozwiązanie testu odbywa się w warunkach kontrolowanej samodzielności, korzystanie z jakichkolwiek pomocy jest niedozwolone, a Komisja może zdyskwalifikować uczestnika w przypadku stwierdzenia niesamodzielności pracy.
3. W każdym zadaniu za każdą prawidłową odpowiedź przyznaje się 1 pkt. Jeśli wybierzesz więcej rozwiązań (zakreślisz więcej odpowiedzi), otrzymasz 0 punktów. Za rozwiązanie testu możesz uzyskać maksymalnie 40 punktów.
4. Po zakończeniu wypełniania testu przenieś odpowiedzi do karty odpowiedzi (na ostatniej stronie arkusza), zamalowując odpowiednie pole. Zrób to uważnie, ponieważ o liczbie zdobytych przez Ciebie punktów z testu decydować będą odpowiedzi zaznaczone w karcie. Nie nanoś żadnych poprawek, nie używaj korektora. Zadania z poprawkami będą oceniane na 0 punktów.
5. Udzielając odpowiedzi na pytania, weź pod uwagę stan na dzień 10 grudnia 2025 r.

Organizator Olimpiady:

WNPiSM UW

UNIWERSYTET WARSZAWSKI

Olimpiada finansowana ze środków:

Ministerstwo Edukacji Narodowej

Patronaty honorowe:

Ministerstwo Obrony Narodowej

Ministerstwo Cyfryzacji

Ministerstwo Spraw Wewnętrznych i Administracji

NASK

1. **Kampania European Cybersecurity Month (ECSM) promująca cyberbezpieczeństwo wśród obywateli i organizacji Unii Europejskiej odbywa się co roku w miesiącu:**
   a) czerwcu
   b) lipcu
   c) październiku
   d) sierpniu

2. **Tailgating w cyberbezpieczeństwie to:**
   a) technika wyłudzania danych przez fałszywe wiadomości e-mail
   b) metoda łamania haseł przez wielokrotne ich zgadywanie
   c) atak polegający na fizycznym dostaniu się do chronionej strefy przez osobę nieuprawnioną, która podąża tuż za osobą z uprawnieniami dostępu
   d) podszywanie się pod inną osobę lub urządzenie w komunikacji sieciowej w celu wyłudzenia danych lub wprowadzenia w błąd

3. **Zgodnie z ustawą z dnia 11 marca 2022 r. o obronie Ojczyzny, Wojska Obrony Terytorialnej to jeden z:**
   a) 3 rodzajów Sił Zbrojnych RP
   b) 4 rodzajów Sił Zbrojnych RP
   c) 5 rodzajów Sił Zbrojnych RP
   d) 6 rodzajów Sił Zbrojnych RP

4. **Afera Cambridge Analytica dotyczyła:**
   a) ataku na infrastrukturę dostawców Internetu w UE
   b) bezprawnego zbierania i wykorzystywania danych użytkowników Facebooka
   c) ataków hackerskich na polityków w USA
   d) działalności grup terrorystycznych w mediach społecznościowych

5. **Do przepisów regulujących poufność informacji zalicza się:**
   a) Ustawę o ochronie informacji niejawnych
   b) Ustawę o ochronie danych poufnych
   c) Ustawę o zasadach udostępniania informacji
   d) Ustawę budżetową

6. **Agencja Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA) to agencja, która:**
   a) zajmuje się rozwojem oprogramowania tworzonego wyłącznie na terenie Unii Europejskiej
   b) prowadzi działania mające na celu osiągnięcie wysokiego wspólnego poziomu cyberbezpieczeństwa w całej Europie
   c) zajmuje się regulacją cen usług internetowych w krajach Unii Europejskiej
   d) odpowiada za przyznawanie patentów technologicznych w Unii Europejskiej

7. **Jednostki tworzące system ratownictwa medycznego i wykonujące medyczne czynności ratunkowe w warunkach pozaszpitalnych w celu ratowania ludzi w stanie nagłego zagrożenia zdrowotnego to:**
   a) lotnicze zespoły ratownictwa medycznego
   b) specjalistyczne zespoły ratownictwa medycznego
   c) podstawowe zespoły ratownictwa medycznego
   d) wszystkie powyższe

8. **Dyrektywa NIS2, w krajach Unii Europejskiej, to dyrektywa w sprawie:**
   a) środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa w całej Unii
   b) ochrony danych osobowych obywateli całej Unii
   c) regulacji dostępu do sieci 5G w całej Unii
   d) ochrony konkurencji na rynku cyfrowym całej Unii

9. **Zgodnie z ustawą z dnia 24 sierpnia 2001 r. o Żandarmerii Wojskowej i wojskowych organach porządkowych, Komendant Główny Żandarmerii Wojskowej podlega bezpośrednio:**
   a) Ministrowi Obrony Narodowej
   b) Prezydentowi RP
   c) Prezesowi Rady Ministrów
   d) Szefowi Sztabu Generalnego Wojska Polskiego

10. **Po otrzymaniu z nieznanego źródła wiadomości SMS lub e-mail o rzekomych zaległościach finansowych, zawierającej link do opłaty, mogącej stanowić próbę oszustwa, zdarzenie takie należy zgłosić do:**
   a) Agencji Bezpieczeństwa Wewnętrznego
   b) Rządowego Centrum Bezpieczeństwa
   c) Zespołu Reagowania na Incydenty Bezpieczeństwa Komputerowego NASK - CSIRT NASK
   d) Ministerstwa Finansów

11. **Siedziba NATO znajduje się w:**
   a) Paryżu
   b) Brukseli
   c) Nowym Jorku
   d) Waszyngtonie

12. **Hakerzy White Hat to:**
   a) hakerzy, którzy działają tylko nocą i zostawiają biały znak po swoich atakach
   b) etyczni hakerzy, wykorzystujący swoje umiejętności na rzecz dobra wspólnego
   c) złodzieje danych, którzy atakują banki i firmy dla zysku
   d) twórcy wirusów komputerowych i programów szpiegowskich

13. **Liczba niestałych członków Rady Bezpieczeństwa ONZ wynosi:**
   a) 5
   b) 8
   c) 10
   d) 12

14. Instytucją w Polsce odpowiedzialną za opracowanie i monitorowanie realizacji Strategii Cyberbezpieczeństwa RP jest:

a) Ministerstwo Cyfryzacji
b) Agencja Rozwoju Strategii Cyberbezpieczeństwa RP
c) Agencja Bezpieczeństwa Wewnętrznego
d) Najwyższa Izba Kontroli

15. Święto Wojska Polskiego jest obchodzone w dniu:

a) 15 sierpnia
b) 24 lipca
c) 4 maja
d) 16 maja

16. Phishing to:

a) specjalny program do usuwania wirusów
b) sposób wykrywania cyberprzestępców
c) próba wyłudzenia danych
d) rodzaj gry online o łowieniu ryb

17. Sekretarzem Generalnym NATO jest:

a) Mark Rutte
b) Jens Stoltenberg
c) Anders Fogh Rasmussen
d) Kaja Kallas

18. Co oznacza skrót „2FA”?

a) punkt darmowego dostępu do sieci WiFi
b) rodzaj wirusa komputerowego
c) dwuskładnikowe uwierzytelnianie
d) system plików

19. Pierwszy i jedyny sąd międzynarodowy powołany do sądzenia osób oskarżanych o popełnienie zbrodni ludobójstwa, przeciwko ludzkości, wojennych i agresji to:

a) Europejski Trybunał Praw Człowieka
b) Międzynarodowy Trybunał Sprawiedliwości
c) Międzynarodowy Trybunał Karny
d) Stały Trybunał Arbitrażowy

20. Najwyższy stopień alarmowy, w wymiarze cyberzagrożeń, zgodnie z nomenklaturą NATO to:

a) CHARLIE
b) ALFA
c) BETA
d) DELTA

21. Ewakuacja realizowana i organizowana natychmiast po wystąpieniu zdarzenia, polegająca na niezwłocznym przemieszczeniu ludności, zwierząt i mienia z miejsc, w których wystąpiło nagłe, nieprzewidziane bezpośrednie zagrożenie poza strefę zagrożenia to ewakuacja:

a) I stopnia
b) II stopnia
c) III stopnia
d) IV stopnia

22. Atak, którego celem jest przeciążenie serwera i zablokowanie dostępu do strony internetowej to:

a) DDoS
b) ransomware
c) malware
d) spoofing

23. Poldery przeciwpowodziowe to:

a) konstrukcje, które buduje się w celu bezpiecznego przeprowadzenia wód wezbraniowych przez określony obszar
b) sztuczne usypiska, najczęściej o trapezowym przekroju, wznoszone wzdłuż rzeki w pewnym oddaleniu od jej koryta
c) naturalne obszary zalewowe, które w okresie wezbrania rzeki pozwalają na swobodne rozlanie się nadmiaru wody
d) sztuczne zbiorniki wodne powstałe w wyniku wybudowania zapory wodnej na rzece i w następstwie zatamowania jej wód

24. Ransomware oznacza:

a) złośliwe oprogramowanie, którego celem jest infiltracja lub uszkodzenie komputera ofiary
b) narzędzie do optymalizacji ustawień systemu operacyjnego
c) proces podszywania się pod inną osobę, urządzenie lub stronę internetową w celu oszukania użytkownika
d) złośliwe oprogramowanie, które szyfruje pliki ofiary i żąda okupu za ich odblokowanie

25. W przypadku krwotoku z nosa:

a) głowę należy pochylić do przodu
b) głowę należy odchylić do tyłu
c) głowę należy na zmianę pochylać do przodu i odchylać do tyłu
d) głową należy potrząsać w lewo i prawo

26. Czym jest „air-gapping”?

a) narzędziem wykradania danych
b) fizycznym odłączeniem sieci od internetu
c) zakłócaniem sygnałów satelitarnych
d) podszywaniem się pod inną osobę w internecie

27. Skrót NASK oznacza:

a) Narodowa Agencja Sieci Komputerowych
b) Naukowa i Akademicka Sieć Komputerowa
c) Naukowa Administracja Sieci Komputerowych
d) Narodowa Administracja Sieci Komputerowych

28. Co jest zagrożeniem przy korzystaniu z publicznych ładowarek USB?

a) niska jakość prądu
b) „Juice Jacking"
c) uszkodzenie baterii
d) utrata gwarancji

29. Szefem Sztabu Generalnego Wojska Polskiego jest generał:

a) Roman Polko
b) Mirosław Różański
c) Rajmund Andrzejczak
d) Wiesław Kukuła

30. Wojska Obrony Cyberprzestrzeni (WOC) zostały utworzone w roku:

a) 2010
b) 2015
c) 2020
d) 2022

31. Cyberwojna to:

a) konflikt pomiędzy grupami ludzi, organizacjami lub państwami oparty na negocjacjach dyplomatycznych i politycznych
b) konflikt pomiędzy grupami ludzi, organizacjami lub państwami prowadzony za pomocą technologii teleinformatycznych
c) idea prowadzenia działań zbrojnych w sieci LAN
d) gra komputerowa polegająca na odtworzeniu klasycznego pola walki w komputerze

32. GOPR to skrót następującej organizacji:

a) Górskie Ochotnicze Pogotowie Ratunkowe
b) Górskie Ochotnicze Pogotowie Ratownicze
c) Górscy Ochotnicy Pogotowia Ratunkowego
d) Góralskie Ochotnicze Pogotowie Ratownicze

33. OSINT, czyli wywiad z otwartych źródeł, oznacza:

a) pozyskiwanie informacji z publicznie dostępnych źródeł w celu analizy i wykorzystania, np. w cyberbezpieczeństwie lub działalności wywiadowczej
b) tworzenie własnych źródeł danych, w tym baz danych offline bez dostępu do internetu
c) prowadzenie rozmów telefonicznych w celu zdobycia poufnych danych
d) pozyskiwanie danych wyłącznie z prywatnych źródeł w celu analizy i wykorzystania, np. w cyberbezpieczeństwie lub działalności wywiadowczej

34. Przesmyk suwalski to terytorium Polski graniczące z:

a) Rosją, Litwą, Białorusią
b) Rosją, Litwą, Białorusią, Ukrainą
c) Ukrainą, Białorusią,
d) Rosją, Łotwą, Białorusią, Ukrainą

35. Deepfake to:

a) dokładne przeszukiwanie systemu w poszukiwaniu wirusów
b) model sztucznej inteligencji wykorzystywany do wykrywania cyberprzestępców
c) wygenerowany przez sztuczną inteligencję fałszywy materiał audio lub wideo
d) pełna kopia zapasowa wszystkich danych firmy

36. Organ opiniodawczo-doradczy działający przy Radzie Ministrów, właściwy w sprawach inicjowania i koordynowania działań podejmowanych w zakresie zarządzania kryzysowego to:

a) Rządowa Komisja Ochrony Ludności i Zarządzania Kryzysowego
b) Rządowa Rada Zarządzania Kryzysowego
c) Rządowy Zespół Zarządzania Kryzysowego
d) Rządowe Centrum Bezpieczeństwa

37. Jaki typ ataku polega na zgadywaniu haseł metodą prób i błędów?

a) Phishing
b) Brute force
c) DDoS
d) Spoofing

38. Zgodnie z konstytucją RP z 1997 r. stanami nadzwyczajnymi, które można przedłużyć są:

a) stan klęski żywiołowej, stan wyjątkowy
b) stan klęski żywiołowej, stan wyjątkowy, stan wojenny
c) stan klęski żywiołowej, stan wyjątkowy, stan wojny
d) stan klęski żywiołowej, stan wojny

39. Jednostką organizacyjną Policji zajmującej się rozpoznawaniem, zapobieganiem i zwalczaniem przestępstw w cyberprzestrzeni jest:

a) CSIRT
b) CBZC
c) Cyber.mil
d) CBŚP

40. Biuro Ochrony Rządu zostało zastąpione przez:

a) Służbę Ochrony Państwa
b) Służbę Ochronną Państwa
c) Agencję Bezpieczeństwa Wewnętrznego
d) Agencję Ochrony Rządu

KARTA ODPOWIEDZI

Nr zadania	Odpowiedź	Liczba punktów
1.	A B C D	
2.	A B C D	
3.	A B C D	
4.	A B C D	
5.	A B C D	
6.	A B C D	
7.	A B C D	
8.	A B C D	
9.	A B C D	
10.	A B C D	
11.	A B C D	
12.	A B C D	
13.	A B C D	
14.	A B C D	
15.	A B C D	
16.	A B C D	
17.	A B C D	
18.	A B C D	
19.	A B C D	
20.	A B C D	
21.	A B C D	
22.	A B C D	
23.	A B C D	
24.	A B C D	
25.	A B C D	
26.	A B C D	
27.	A B C D	
28.	A B C D	
29.	A B C D	
30.	A B C D	
31.	A B C D	
32.	A B C D	
33.	A B C D	
34.	A B C D	
35.	A B C D	
36.	A B C D	
37.	A B C D	
38.	A B C D	
39.	A B C D	
40.	A B C D	

Łączna liczba punktów: ……/40

Podpisy członków Komisji:

Przewodniczący ….…….

Członek Komisji …….

Członek Komisji …….