UNIWERSYTET WARSZAWSKI

DZIENNIK UNIWERSYTETU WARSZAWSKIEGO
RADY DYDAKTYCZNE DLA KIERUNKÓW STUDIÓW

UCHWAŁA NR 19/2026
RADY DYDAKTYCZNEJ DLA KIERUNKÓW STUDIÓW BEZPIECZEŃSTWO WEWNĘTRZNE, CYBERBEZPIECZEŃSTWO, EUROPEISTYKA – INTEGRACJA EUROPEJSKA, ORGANIZOWANIE RYNKU PRACY, POLITOLOGIA, POLITYKA KULTURALNA I ZARZĄDZANIE W KULTURZE, POLITYKA PUBLICZNA, POLITYKA SPOŁECZNA, STOSUNKI MIĘDZYNARODOWE, STUDIA EUROAZJATYCKIE

z dnia 4 maja 2026 r.

w sprawie zasad rekrutacji na rok akademicki 2027/2028 na studia II stopnia na kierunku cyberbezpieczeństwo oraz harmonogramu rekrutacji na rok akademicki 2027/2028 na studia II stopnia na kierunku cyberbezpieczeństwo

Na podstawie § 68 ust. 2 Statutu Uniwersytetu Warszawskiego (Monitor UW z 2019 r. poz. 190) oraz § 5 ust. 1 pt. 2 Regulaminu studiów na Uniwersytecie Warszawskim (Monitor UW z 2019 r. poz. 186) Rada Dydaktyczna postanawia, co następuje:

§ 1

Rada Dydaktyczna proponuje zasady rekrutacji na rok akademicki 2027/2028 na studia II stopnia na kierunku cyberbezpieczeństwo zgodne z załącznikiem nr 1 do uchwały.

§ 2

Rada Dydaktyczna proponuje harmonogram rekrutacji na rok akademicki 2027/2028 na studia II stopnia na kierunku cyberbezpieczeństwo zgodnie z załącznikiem nr 2.

§ 3

Uchwała wchodzi w życie z dniem podjęcia.

Przewodniczący Rady Dydaktycznej: *T. Mering*

Załącznik nr 1
do uchwały nr 19/2026 Rady Dydaktycznej dla kierunków studiów: bezpieczeństwo wewnętrzne, cyberbezpieczeństwo, europeistyka-integracja europejska, organizowanie rynku pracy, politologia, polityka kulturalna i zarządzanie w kulturze, polityka publiczna, polityka społeczna, stosunki międzynarodowe, studia euroazjatyckie z dnia 4 maja 2026 r. w sprawie propozycji zasad rekrutacji otwartej na rok akademicki 2027/2028 na studia II stopnia na kierunku cyberbezpieczeństwo

ZASADY REKRUTACJI OTWARTEJ

Kierunek studiów: cyberbezpieczeństwo
Poziom kształcenia: drugiego stopnia
Profil kształcenia: ogólnoakademicki
Forma studiów: stacjonarne
Czas trwania: 2 lata

1) Zasady kwalifikacji

Próg kwalifikacji: 20 pkt.

a) Kandydaci z dyplomem uzyskanym w Polsce

Podstawą kwalifikacji jest **egzamin testowy**, składający się z pytań zamkniętych oraz otwartych, przeprowadzany z zakresu podanej literatury do egzaminu oraz następujących zagadnień:

Zagadnienia:

1. Sposoby ochrony komputera osobistego przed cyberprzestępcami.
2. Zagrożenia bezpieczeństwa wynikające z korzystania z mediów społecznościowych.
3. Istota cyberwojny.
4. Możliwe konsekwencje społeczne wynikające z braku działania:
   - Internetu,
   - sieci społecznościowych,
   - serwisów informacyjnych.
5. Powszechnie znane wycieki danych osobowych w sieciach komputerowych. Istota i środki zaradcze podjęte w celu ograniczenia ryzyka ich wystąpienia w przyszłości.
6. Zasady bezpiecznego korzystania z usług bankowości elektronicznej w Polsce.
7. Prawo do zapomnienia.
8. Sposoby zabezpieczenia smartfonu przed atakami cyberprzestępców.
9. Korzyści wynikające z używania legalnie nabytego oprogramowania komputerowego.
10. Możliwe konsekwencje korzystania z niezabezpieczonej sieci Wi-Fi.

Literatura:

- Aleksandrowicz T.R., Zagrożenia dla bezpieczeństwa informacyjnego państwa w ujęciu systemowym: budowanie zdolności defensywnych i ofensywnych w infosferze, Warszawa 2021.
- Widawski P., Szpyra R., Mednis A., i in. (red.), Cyberbezpieczeństwo: zarys wykładu, Warszawa 2023.
- Brotherston L., Berlin A., Lachowski L., Grupa Wydawnicza Helion, Bezpieczeństwo defensywne: podstawy i najlepsze praktyki, Gliwice 2019
- Dela P., Założenia działań w cyberprzestrzeni, Warszawa 2022.
- Cunningham C., Kowalczyk G., Wojny w cyberprzestrzeni: koncepcje, strategie i taktyki dzięki którym przetrwasz i ocalisz swoją organizację, Gliwice 2021.
- Gray J., Wyrodow-Rakowski P., Grupa Wydawnicza Helion, Socjotechniki w praktyce: podręcznik etycznego hakera, Gliwice 2023.
- Kowalczyk M., Cyfrowe Państwo: uwarunkowania i perspektywy, Warszawa 2019.
- Liderman K., Wydawnictwo Naukowe PWN, Bezpieczeństwo informacyjne: nowe wyzwania, Warszawa 2017.

- Kowalewski M., Jakubiak M. (red.), Cyberprzemoc szczególnym zagrożeniem społeczeństwa informacyjnego, Warszawa 2021.
- Olejnik Ł., Kurasiński A. (red.), Filozofia cyberbezpieczeństwa: jak zmienia się świat?: od złośliwego oprogramowania do cyberwojny, Warszawa 2022.
- Sanger D.E., Misiorek T., Cyberbroń - broń doskonała: wojny, akty terroryzmu i zarządzanie strachem w epoce komputerów, Gliwice 2021.
- Publikacje CERT Polska dostępne na stronie https://cert.pl/publikacje/

Wynik końcowy to liczba punktów w przedziale od 0 do 50.

b) Kandydaci z dyplomem zagranicznym

Obowiązują takie same zasady, jak dla kandydatów z dyplomem uzyskanym w Polsce.

2) Sprawdzenie kompetencji kandydatów do studiowania w języku polskim

Kandydaci z dyplomem zagranicznym, aplikujący na studia prowadzone w języku polskim, są zobowiązani dodatkowo do poświadczenia znajomości języka polskiego.

Kompetencje językowe kandydatów sprawdzane są zgodnie z zasadami określonymi w uchwale Senatu wraz z załącznikami.

Kandydaci, którzy nie legitymują się dokumentem poświadczającym znajomość języka polskiego i nie są wymienieni w załączniku nr 4 do uchwały będą mieli możliwość potwierdzenia znajomości tego języka na poziomie co najmniej B2 podczas sprawdzianu znajomości języka polskiego.

Sprawdzian znajomości języka polskiego będzie miał formę rozmowy.

Rozmowa będzie dotyczyła aktualnych wydarzeń politycznych, społecznych i ekonomicznych.

Podczas rozmowy kandydat może uzyskać maksymalnie 30 punktów w wyniku oceny:
- zasobu słownictwa – 0-10 pkt.
- poprawności gramatycznej wypowiedzi – 0-10 pkt.
- języka, stylu i kompozycji wypowiedzi – 0-10 pkt.

Próg kwalifikacji: 16 pkt.

W dalszej kwalifikacji brani są pod uwagę wyłącznie kandydaci, którzy potwierdzili znajomość języka polskiego na poziomie co najmniej B2.

Brak poświadczenia przez kandydata znajomości języka polskiego na poziomie co najmniej B2 powoduje przyznanie 0 (zera) punktów z całości postępowania kwalifikacyjnego i dyskwalifikację kandydata.

Punktacja za rozmowę sprawdzającą znajomość języka polskiego nie jest wliczana do punktacji końcowej.

Załącznik nr 2
do uchwały nr 19/2026 Rady Dydaktycznej dla kierunków studiów: bezpieczeństwo wewnętrzne, cyberbezpieczeństwo, europeistyka-integracja europejska, organizowanie rynku pracy, politologia, polityka kulturalna i zarządzanie w kulturze, polityka publiczna, polityka społeczna, stosunki międzynarodowe, studia euroazjatyckie z dnia 4 maja 2026 r. w sprawie propozycji harmonogramu rekrutacji otwartej na rok akademicki 2027/2028 na studia II stopnia na kierunku cyberbezpieczeństwo

HARMONOGRAM REKRUTACJI OTWARTEJ

Kierunek studiów: cyberbezpieczeństwo
Poziom kształcenia: drugiego stopnia
Profil kształcenia: ogólnoakademicki
Forma studiów: stacjonarne
Czas trwania: 2 lata

Tura rekrutacji	Początek rejestracji	Koniec rejestracji	Egzamin wstępny**	Zatwierdzenie wyników	Ogłoszenie wyników	Przyjmowanie dokumentów
I tura	09.06.2027	20.07.2027	27.07.2027	30.07.2027	02.08.2027	I termin: 03-05.08.2027 w przypadku niewypełnienia limitu miejsc: II termin: 06, 09.08.2027 w przypadku niewypełnienia limitu miejsc: III termin: 10-11.08.2027 kolejne terminy wyznaczone przez komisję rekrutacyjną
II tura*	19.08.2027	10.09.2027	15.09.2027	22.09.2027	23.09.2027	I termin: 24, 27.09.2027 w przypadku niewypełnienia limitu miejsc: II termin: 28-29.09.2027

** w przypadku niewypełnienia limitu miejsc w I turze*
*** w tym sprawdzian znajomości języka polskiego (o ile dotyczy kandydata)*