„ZATWIERDZAM”
DYREKTOR
DEPARTAMENTU CYBERBEZPIECZEŃSTWA
25.09.2024 r.
.....
Dominik RÓŻYCKI-WOWSKI
(podpis, data)

REGULAMIN

Projektu Akademia_CYBER.MIL w roku akademickim 2024/2025

§ 1. Postanowienia ogólne dotyczące realizacji Projektu

1. Podstawą wdrożenia Projektu Akademia_CYBER.MIL (dalej: Projekt) jest niepublikowana *Decyzja Nr 316/DC Ministra Obrony Narodowej z dnia 22 sierpnia 2024 r. w sprawie realizacji Projektu Akademia_CYBER.MIL w roku akademickim 2024/2025*, dotycząca wsparcia cywilnych uczelni w procesie kształcenia na kierunkach związanych z cyberbezpieczeństwem, IT i łącznością.
2. Organizatorem Projektu jest Ministerstwo Obrony Narodowej, reprezentowane przez Departament Cyberbezpieczeństwa i Eksperckie Centrum Szkolenia Cyberbezpieczeństwa (dalej: Organizatorzy).
3. Celem Projektu jest popularyzowanie wizerunku Sił Zbrojnych Rzeczypospolitej Polskiej oraz jednostek organizacyjnych resortu obrony narodowej, jako atrakcyjnego i innowacyjnego miejsca do podjęcia pracy i służby oraz rozwoju kariery zawodowej dla ekspertów w dziedzinie cyberbezpieczeństwa, IT i łączności, w tym w szczególności popularyzowanie wiedzy, budowanie świadomości o zagrożeniach oraz zainteresowanie studentów szeroko rozumianym obszarem cyberbezpieczeństwa.
4. W ramach Projektu zakłada się udostępnienie dla studentów uczelni biorących udział w Projekcie, o których mowa w **Załączniku nr 1 do Regulaminu**, na wydzielonej platformie e-learningowej, certyfikowanych kursów z obszaru cyberbezpieczeństwa w okresie od listopada 2024 r. do lutego 2025 r.
5. Kursy udostępnione będą wg poniższego harmonogramu:
   1) Kurs pn.: „Akademia Bezpieczeństwa” — w okresie od 4 do 22 listopada 2024 r.;
   2) Kurs pn.: „Bezpieczeństwo systemu Windows” — w okresie od 2 do 20 grudnia 2024 r.;
   3) Kurs pn.: „Bezpieczeństwo systemu Linux” — w okresie od 6 do 23 stycznia 2025 r.;
   4) Kurs pn.: „Ekspert bezpieczeństwa OSSTMM” — w okresie od 3 do 21 lutego 2025 r.
6. Każdy z kursów zakończony będzie testem wiedzy, do którego można podejść maksymalnie dwa razy. Do zaliczenia testu konieczne jest udzielenie 70% poprawnych odpowiedzi.
7. Po uzyskaniu pozytywnego wyniku z testu wiedzy po każdym z kursów będzie możliwość wygenerowania zaświadczenia o jego ukończeniu po wcześniejszym wypełnieniu ankiety satysfakcji.
8. Zainteresowani studenci będą mieli możliwość wzięcia udziału w dowolnej liczbie kursów.
9. Projekt skierowany jest do studentów posiadających obywatelstwo polskie.
10. Studenci zainteresowani wzięciem udziału w Projekcie zgłaszają się do wyznaczonego przez Rektora koordynatora uczelnianego. Informację w tej sprawie posiada Biuro Karier na uczelni.

11. Zbiorczą listę studentów z danej uczelni, w formie tabelarycznej wg wzoru określonego w **Załączniku nr 2 do Regulaminu**, koordynator uczelniany przesyła w terminie do dnia 23 października 2024 r. do Departamentu Cyberbezpieczeństwa MON.
12. Przed terminem udostępnienia danego kursu na platformie e-learningowej, na wskazane przez studentów zgłoszonych do udziału w Projekcie adresy e-mail z domeną uczelni, zostaną przesłane linki z instrukcją dostępu do danego kursu, który można realizować w częściach, przez cały okres jego trwania, zgodnie z harmonogramem, o którym mowa w pkt 5.
13. Na zakończenie Projektu w dniu 3 marca 2025 r. zorganizowane zostaną ogólnopolskie zawody Capture The Flag (dalej: CTF).

§ 2. Zasady organizacji ogólnopolskich zawodów CTF

1. Organizatorem CTF jest Ministerstwo Obrony Narodowej, reprezentowane przez Departament Cyberbezpieczeństwa i Eksperckie Centrum Szkolenia Cyberbezpieczeństwa (dalej: Organizatorzy).
2. CTF odbędzie się w dniu 3 marca 2025 r. w Centrum Konferencyjnym Wojska Polskiego (ul. Żwirki i Wigury 9/13, 02-143 Warszawa). Oficjalne rozpoczęcie CTF nastąpi o godz.: 8:00
3. W dniu zawodów należy stawić się w miejscu wskazanym w pkt 2 o godz.: 7:00, z dokumentem potwierdzającym tożsamość.
4. Organizatorzy zastrzegają sobie prawo do zmiany terminu CTF, jeśli taka zmiana będzie uzasadniona względami organizacyjnymi.
5. Przyjazd na CTF i ewentualny nocleg uczestnicy organizują we własnym zakresie.
6. W dniu CTF uczestnicy będą mieli zapewnione całodzienne bezpłatne wyżywienie.
7. Zawody CTF skierowane są do studentów uczelni zakwalifikowanych do udziału w Projekcie.
8. Każda uczelnia wystawia jeden czteroosobowy zespół.
9. Każdy zespół może wycofać się z CTF w dowolnym czasie. Wycofanie jest równoznaczne z utratą prawa do nagród, o których mowa w pkt 40-41.
10. Ustalenie składu zespołów biorących udział w CTF pozostawia się w gestii władz poszczególnych uczelni.
11. Warunkiem uczestnictwa w CTF jest:
    1) ukończenie przez studenta w dniu rozpoczęcia zawodów 18 lat;
    2) posiadanie obywatelstwa polskiego;
    3) posiadanie pełnej zdolność do czynności prawnych
    (wzór Oświadczenia określony w **Załączniku nr 3 do Regulaminu**);
12. Przed przystąpieniem do udziału w CTF uczestnik powinien zapoznać się z niniejszym Regulaminem dostępnym u koordynatorów uczelnianych Projektu oraz na stronie internetowej www.ecsc.mil.pl.
13. Udział w CTF jest równoznaczny z akceptacją Regulaminu.
14. W terminie do dnia 15 lutego 2025 r. uczelnie prześlą do Departamentu Cyberbezpieczeństwa MON dane osób wchodzących w skład zespołów, zgodnie ze wzorem określonym w **Załączniku nr 4 do Regulaminu.**
15. Weryfikacji uczestników zawodów dokona Departament Cyberbezpieczeństwa MON.
16. Podanie organizatorom CTF danych, o których mowa w pkt 14 warunkuje udział w zawodach CTF.
17. Brak akceptacji Oświadczenia (o którym mowa w pkt 11), uniemożliwia zgłoszenie i udział w CTF.

18. Podczas CTF członkowie zespołów otrzymają jednorazowe kody pozwalające na założenie konta na dedykowanej platformie i udział w rozwiązywaniu zadań konkursowych.
19. W ramach CTF zespoły będą rywalizowały między sobą, gromadząc punkty w różnych konkurencjach na konto swojej drużyny na dedykowanej platformie, która zostanie udostępniona w dniu zawodów. Dodatkowo punkty można będzie zdobyć w konkurencjach sportowych, o których mowa w pkt 26.
20. Organizatorzy zapewnią uczestnikom dostęp do sieci komputerowej (m.in. Wi-Fi).
21. Organizatorzy zapewnią dostęp do platformy wymienionej w pkt 18 dla każdego członka zespołu.
22. Momentem rozpoczęcia CTF jest oficjalne przedstawienie treści zadań podczas otwarcia zawodów. Dopiero od tego momentu możliwe jest zapoznanie się przez zespoły z treścią zadań i rozpoczęcie ich rozwiązywania.
23. Po zapoznaniu się z tematem zadań i ogłoszeniem otwarcia CTF, każdy z uczestników otrzyma instrukcję wykonywania zadań wraz z ich punktacją. CTF będzie trwał maksymalnie 8 godzin.
24. Organizatorzy zastrzegają sobie prawo modyfikacji zadań. Każdy zespół będzie powiadomiony o wprowadzonej modyfikacji w celu doprecyzowania lub naprawienia błędu w zadaniu poprzez platformę wymienioną w pkt 18.
25. Aby rozwiązać zadanie należy znaleźć ukrytą flagę - specjalny ciąg znaków udowadniający rozwiązanie zadania lub wykonać określone czynności zmierzające do udzielenia odpowiedzi na pytanie. Za zgłoszenie za pomocą platformy (wymienionej w pkt 18) flagi lub odpowiedzi uczestnicy dostają punkty. Znalezienie i zgłoszenie flagi lub udzielenie odpowiedzi na pytanie jest celem każdego zadania.
26. Dodatkowo poza zadaniami wskazanymi przez Organizatorów do wykonania przy stanowiskach komputerowych w ramach CTF, zespoły będą miały możliwość zdobycia dodatkowych punktów w rywalizacjach sportowych (na strzelnicy wirtualnej, rzutkach, rowerze stacjonarnym, tenisie stołowym i wioślarzu - szczegóły na miejscu). Punkty te będą brane pod uwagę w przypadku zdobycia przez drużyny równej liczby punktów we właściwych zawodach CTF realizowanych przy stanowiskach komputerowych.
27. Organizatorzy zawodów zapewnią uczestnikom kanał komunikacyjny (np. czat) umożliwiający zgłaszanie problemów z platformą i zadaniami w czasie trwania CTF.
28. Uczestnicy CTF zobowiązują się wykonać zadania stanowiące przedmiot zawodów samodzielnie i bez pomocy z zewnątrz.
29. Uczestnikom CTF nie wolno, pod rygorem natychmiastowego wykluczenia z udziału w zawodach, podejmować prób uzyskania dostępu do treści zadania przed rozpoczęciem CTF.
30. Organizatorzy mają prawo wykluczyć zespół z CTF, jeżeli stwierdzą złamanie postanowień Regulaminu lub przepisów prawa powszechnie obowiązującego np.: ataki na infrastrukturę teleinformatyczną, niszczenie infrastruktury, niszczenie zadań lub utrudnianie rozwiązywania ich przez uczestników innych zespołów.
31. Organizatorzy CTF określą skład trzyosobowej Komisji oceniającej zawody.
32. Komisja oceniająca ze swego grona wybierze przewodniczącego.
33. Komisja dokona oceny zadań realizowanych przez poszczególne Zespoły, z czego sporządzi protokół oraz ogłosi wyniki zawodów CTF.
34. Zakres wiedzy uczestników CTF nie podlega ocenie przez Komisję oceniającą.

35. Decyzja Komisji oceniającej jest ostateczna i nie podlega odwołaniu.
36. Wyznaczone przez Organizatorów osoby zapewnią doraźną pomoc techniczną podczas trwania CTF (wsparcie techniczne oraz merytoryczne, bez podpowiedzi odnośnie do sposobu rozwiązywania zadań - dla uczestników w zakresie platformy).
37. Rozstrzygnięcie CTF nastąpi w dniu 3 marca 2025 r.
38. Zwycięzcy CTF zostaną powiadomieni o wynikach zawodów w formie ustnej.
39. Za uczestnictwo w CTF dla wszystkich uczestników przewidziane są dyplomy.
40. Zespoły, które zajmą I, II i III miejsce w CTF, otrzymają od Organizatorów zaproszenie na Międzynarodowy Kongres Cyberbezpieczeństwa INSECON, organizowany przez Departament Cyberbezpieczeństwa MON na Międzynarodowych Targach Poznańskich, w terminie 2-3 kwietnia 2025 r.
41. Zwycięzcy CTF otrzymają szczególną nagrodę w postaci pakietu przygotowanego przez Akademię Marynarki Wojennej im. Bohaterów Westerplatte z siedzibą w Gdyni obejmującego wizytę i zwiedzanie gmachu AMW, zwiedzanie Portu Wojennego w Gdyni oraz rejs łodzią motorową po Zatoce Gdańskiej.
42. Warunkiem wydania nagród jest obecność podczas ogłaszania wyników zawodów CTF. Brak obecności powoduje utratę nagrody.
43. Laureaci mają prawo do rezygnacji z przyjęcia nagrody.
44. Wydarzenia stanowiące nagrody, o których mowa w pkt 40-41, odbędą się w miejscu, czasie i na warunkach ustalonych przez Organizatorów.
45. Uczestnicy CTF są zobowiązani do zachowania w poufności treści zadań zawodów oraz informacji, wiedzy, danych, jak również dokumentów i ich projektów udostępnionych przez Organizatorów lub opracowanych i/lub przygotowanych przez uczestników CTF.
46. W celu uniknięcia jakichkolwiek wątpliwości Organizatorzy informują, że użyte w Regulaminie określenie *Informacje chronione* nie dotyczy informacji niejawnych w rozumieniu *Ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (tj. Dz. U. z 2019 poz. 412 ze zm.).*
47. Informacje chronione to treści zadań zawodów, informacje, wiedza, dane, jak również dokumenty i projekty dokumentów (także w postaci nieukończonej) udostępnione przez Organizatorów lub opracowane/przygotowane przez uczestników CTF w czasie ich trwania oraz 12 miesięcy po ich zakończeniu. To również informacje o charakterze technicznym, technologicznym (w tym dokumenty, oprogramowanie, dane), lub inne informacje uzyskane w wyniku analizy, lub przetworzenia dostarczonych informacji (w tym danych osobowych) oraz które:
    1) nie zostały podane do publicznej wiadomości,
    2) które uczestnicy CTF uzyskali i/lub które mogą stać się im znane w toku rozmów i/lub w związku z wykonywaniem przez uczestników zawodów CTF.
48. Informacje chronione będą wykorzystywane przez uczestnika CTF wyłącznie w celu udziału w zawodach.
49. Organizatorzy informują, że zobowiązanie do zachowania w poufności Informacji chronionych obejmuje m.in.:
    1) zakaz rozpowszechniania, kopiowania lub dystrybucji, ujawniania, przekazywania, potwierdzania i/lub składania komentarzy dotyczących Informacji chronionych wobec osób i podmiotów trzecich i/lub nieupoważnionych osób, pośrednio bądź bezpośrednio;

2) obowiązek niezwłocznego poinformowania Organizatorów o fakcie utraty, ujawnienia lub powielenia Informacji chronionej i/lub niedotrzymania warunków Regulaminu.

50. Uczestnik CTF zobowiązuje się zwrócić Organizatorom wszelkie urządzenia, dokumenty (włączając ich kopie) oraz nośniki danych niezwłocznie po ich wykorzystaniu lub użyciu dla realizacji zawodów, oraz usunąć dane i informacje zapisane w pamięci komputera lub na innych nośnikach danych.
51. Organizatorzy zastrzegają sobie prawo odwołania lub zakończenia CTF przed czasem bez podania przyczyny.
52. Organizatorzy zastrzegają sobie prawo do dokonania zmian w Regulaminie bez konsultacji z uczestnikami CTF.
53. CTF zostanie zakończony uroczystym wręczeniem dyplomów i nagród oraz bankietem z udziałem kierownictwa MON i zaproszonych gości.

§ 3. Ochrona danych osobowych

1. Administratorem danych osobowych uczestników biorących udział w Projekcie Akademia_CYBER.MIL w rozumieniu art. 13 *Rozporządzenia Parlamentu Europejskiego i Rady (DE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE* jest Minister Obrony Narodowej z siedzibą w Warszawie, przy al. Niepodległości 218.
2. Klauzula informacyjna RODO stosowana przy Projekcie Akademia_CYBER.MIL w roku akademickim 2024/2025 wobec koordynatorów oraz studentów uczelni biorących w nim udział stanowi **Załącznik nr 5 do Regulaminu.**

Załącznik nr 1 do Regulaminu

Wykaz uczelni zakwalifikowanych do udziału w Projekcie Akademia_CYBER.MIL w roku akademickim 2024/2025

1. Akademia Górniczo-Hutnicza im. Stanisława Staszica w Krakowie
2. Politechnika Białostocka
3. Politechnika Bydgoska im. Jana i Jędrzeja Śniadeckich
4. Politechnika Gdańska
5. Politechnika Koszalińska
6. Politechnika Krakowska im. Tadeusza Kościuszki
7. Politechnika Lubelska
8. Politechnika Łódzka
9. Politechnika Opolska
10. Politechnika Poznańska
11. Politechnika Rzeszowska im. Ignacego Łukasiewicza
12. Politechnika Śląska
13. Politechnika Świętokrzyska
14. Politechnika Wrocławska
15. Uniwersytet Radomski im. Kazimierza Pułaskiego
16. Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Załącznik nr 2 do Regulaminu

.....
(nazwa uczelni

/Wzór/

Zgłoszenie uczestników do Projektu Akademia_CYBER.MIL

Lp.	Imię	Nazwisko	e-mail z domeną uczelni	Nazwa kierunku studiów	Rok studiów	Nazwa kursu			
						Akademia Bezpieczeństwa	Bezpieczeństwo systemu Windows	Bezpieczeństwo systemu Linux	Ekspert bezpieczeństwa OSSTMM

Załącznik nr 3 do Regulaminu

OŚWIADCZENIE

uczestnika ogólnopolskich zawodów Capture The Flag

Ja *(imię i nazwisko)* .....

Student *(nazwa uczelni)* .....

na kierunku .....

oświadczam, iż:

1. Jestem pełnoletnia/ni i posiadam pełną zdolność do czynności prawnych.
2. Posiadam obywatelstwo polskie.
3. Akceptuję zapisy Regulaminu Projektu Akademia_CYBER.MIL oraz zobowiązuję się do ich przestrzegania.
4. Zobowiązuję się do zachowania poufności w zakresie określonym w Regulaminie.

.....
(podpis studenta)

5. Wyrażam zgodę na dokumentowanie i utrwalanie wybranych przez Organizatorów zdarzeń w ramach CTF, włącznie z rejestrowaniem dźwięku i obrazu, a w szczególności utrwalania mojego wizerunku w celu późniejszego wykorzystania tych materiałów do celów związanych z informowaniem przez Organizatorów o przebiegu CTF i jego wyniku.

.....
(podpis studenta)

Załącznik nr 4 do Regulaminu

.....

(nazwa uczelni)

Skład zespołu
do udziału w Ogólnopolskich Zawodach Capture The Flag
w ramach Projektu Akademia_CYBER.MIL realizowanych w roku akademickim 2024/2025

Lp.	Imię	Nazwisko	e-mail z domeną uczelni	Nazwa kierunku studiów	Rok studiów
1.					
2.					
3.					
4.					

Załącznik nr 5 do Regulaminu

KLAUZULA INFORMACYJNA RODO

stosowana przy Projekcie Akademia_CYBER.MIL w roku akademickim 2024/2025
wobec koordynatorów oraz studentów uczelni biorących w nim udział

Działając na podstawie art. 14 ust. 1 i 2 RODO, informuję Panią/Pana, że: administratorem danych osobowych jest Minister Obrony Narodowej z siedzibą w Warszawie, przy al. Niepodległości 218, e-mail: dc.sekretariat@mon.gov.pl.

Administrator wyznaczył Inspektora Ochrony Danych, z którym można się kontaktować poprzez pocztę elektroniczną na adres: iod@mon.gov.pl lub listownie na adres: Ministerstwo Obrony Narodowej, al. Niepodległości 218, 00-911 Warszawa, z dopiskiem „Inspektor Ochrony Danych".

Pani/Pana dane osobowe, tj.: imię i nazwisko, nazwa uczelni, e-mail z domeną uczelni, nazwa kierunku studiów (w przypadku studentów) oraz rok studiów (w przypadku studentów), pozyskane zostały z (nazwa uczelni) ..... i przetwarzane będą w celu zrealizowania *Decyzji Nr 316/DC Ministra Obrony Narodowej z dnia 22 sierpnia 2024 r. w sprawie realizacji Projektu Akademia_CYBER.MIL w roku akademickim 2024/2025*, która służy administratorowi do wykonania zadania realizowanego w interesie publicznym.

Podstawą prawną przetwarzania danych osobowych jest art. 6 ust. 1 lit. e RODO w związku z art. 2 pkt 1 i pkt 23 *ustawy z dnia 14 grudnia 1995 r. o urzędzie Ministra Obrony Narodowej (Dz. U. z 2022 r. poz. 1438)*, § 2 pkt 3a *rozporządzenia Rady Ministrów z dnia 9 lipca 1996 r. w sprawie szczegółowego zakresu działania Ministra Obrony Narodowej (Dz. U. poz. 426 oraz z 2014 r. poz. 933)* oraz ww. *Decyzją Nr 316/DC Ministra Obrony Narodowej*, tj. przetwarzanie danych jest niezbędne do wykonania zadania realizowanego w interesie publicznym.

Dane osobowe będą przekazywane podmiotom przetwarzającym dane osobowe na zlecenie administratora, a także innym podmiotom uprawnionym na podstawie przepisów prawa, w tym podmiotom współrealizującym Projekt Akademia_CYBER.MIL, tj.: Dowództwu Komponentu Wojsk Obrony Cyberprzestrzeni, Eksperckiemu Centrum Szkolenia Cyberbezpieczeństwa i Wojskowemu Centrum Edukacji Obywatelskiej.

Dane nie będą przekazywane do państwa trzeciego ani do organizacji międzynarodowej.

Dane będą przechowywane przez okres 10 lat wynikający z przepisów prawa, tj. zgodnie z obowiązującym w Ministerstwie Obrony Narodowej „Jednolitym Rzeczowym Wykazem Akt".

Osobie, której dane dotyczą, przysługuje prawo do:

- dostępu do danych osobowych; żądania ich sprostowania; ograniczenia przetwarzania, w przypadkach wymienionych w RODO,
- wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych (adres: 00-193 Warszawa, ul. Stawki 2).

Osobie, której dane dotyczą, nie przysługuje prawo do: przenoszenia danych, usunięcia danych, wniesienia sprzeciwu.

Informuję, że prawo do sprzeciwu nie przysługuje Pani/Panu ze względu na to, że istnieją ważne, prawnie uzasadnione podstawy do przetwarzania Pani/Panu danych.

W trakcie przetwarzania danych nie będzie dochodziło do zautomatyzowanego podejmowania decyzji ani do profilowania.