Warszawa, dnia 23 czerwca 2021 r.

Poz. 150

ZARZĄDZENIE Nr 59/MON
MINISTRA OBRONY NARODOWEJ

z dnia 23 czerwca 2021 r.

w sprawie przyjęcia Programu CYBER.MIL z klasą

Na podstawie art. 2 pkt 2, 5 i 22 ustawy z dnia 14 grudnia 1995 r. o urzędzie Ministra Obrony Narodowej (Dz. U. z 2019 r. poz. 196) i art. 51 pkt 3 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2020 r. poz. 1369), zarządza się, co następuje:

§ 1. Przyjmuje się Program CYBER.MIL z klasą, stanowiący załącznik do zarządzenia.

§ 2.1. Szkoły zakwalifikowane do Programu CYBER.MIL z klasą na podstawie dotychczasowych przepisów pozostają w Programie CYBER.MIL z klasą.

2. W sprawach postępowań będących w toku i dotyczących szkół zakwalifikowanych do Programu CYBER.MIL z klasą stosuje się przepisy określone w załączniku do zarządzenia.

§ 3. Traci moc zarządzenie Nr 12/MON Ministra Obrony Narodowej z dnia 23 kwietnia 2020 r. w sprawie wdrożenia „Programu CYBER.MIL z klasą” (Dz. Urz. Min. Obr. Nar. poz. 73).

§ 4. Zarządzenie wchodzi w życie z dniem ogłoszenia.

Minister Obrony Narodowej: z up. *W. Skurkiewicz*

Załącznik do zarządzenia Nr 59/MON
Ministra Obrony Narodowej
z dnia 23 czerwca 2021 r. (poz. 150)

Program CYBER.MIL z klasą

Rozdział I. Postanowienia ogólne

1. Program CYBER.MIL z klasą, zwany dalej „Programem”, opracowano w celu wsparcia obronności państwa poprzez kształcenie i przygotowanie profesjonalnych kadr w obszarze bezpieczeństwa informatycznego i teleinformatycznego na potrzeby jednostek organizacyjnych resortu obrony narodowej.
2. Program oznacza realizację projektu Ministra Obrony Narodowej, polegającego na utworzeniu i prowadzeniu, w ramach działalności innowacyjnej, w wyłonionych 16 szkołach ponadpodstawowych na terenie kraju, zwanych dalej „szkołami”, oddziałów szkolnych realizujących Program w obszarze cyberbezpieczeństwo i nowoczesne technologie informatyczne, zwanych dalej „oddziałami cyberbezpieczeństwa”.
3. Program zakłada edukowanie zakwalifikowanych uczniów w zakresie rozszerzonej informatyki z uwzględnieniem zagadnień dotyczących cyberbezpieczeństwa, w szczególności obronności państwa w rozumieniu zadań resortu obrony narodowej.
4. Program ustala cel główny i cele szczegółowe projektu, wykonawców, uczestników, okres realizacji, założenia organizacyjne, finansowanie oraz sposób oceny i ewaluacji projektu, a także warunki uczestnictwa szkół oraz doboru uczniów do udziału w Programie.

Rozdział II. Podstawy prawne

Problematykę zawartą w Programie regulują akty prawne, w szczególności:
1) ustawa z dnia 27 sierpnia 2009 r. o finansach publicznych (Dz. U. z 2021 r. poz. 305);
2) ustawa z dnia 14 grudnia 2016 r. – Prawo oświatowe (Dz. U. z 2020 r. poz. 910 i 1378 oraz z 2021 r. poz. 4, 619 i 762);
3) ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2020 r. poz. 1369);
4) ustawa z dnia 27 października 2017 r. o finansowaniu zadań oświatowych (Dz. U. z 2020 r. poz. 2029 i 2400 oraz z 2021 r. poz. 619);
5) ustawa z dnia 20 lipca 2018 r. – Prawo o szkolnictwie wyższym i nauce (Dz. U. z 2021 r. poz. 478 i 619);
6) decyzja Nr 122/MON Ministra Obrony Narodowej z dnia 20 września 2018 r. w sprawie planowania i wykonywania budżetu resortu obrony narodowej (Dz. Urz. Min. Obr. Nar. poz. 149, z 2019 r. poz. 256 oraz z 2021 r. poz. 8);
7) decyzja budżetowa na rok 2021 Nr 7/MON Ministra Obrony Narodowej z dnia 10 lutego 2021 r. (Dz. Urz. Min. Obr. Nar. poz. 10, 89, 108, 124 i 132).

Rozdział III. Cel główny i cele szczegółowe Programu

1. Celem głównym Programu jest zbudowanie bazy naboru do korpusów osobowych kadry

zawodowej i naukowej Sił Zbrojnych Rzeczypospolitej Polskiej na potrzeby jednostek organizacyjnych resortu obrony narodowej, w tym planowanych do utworzenia Wojsk Obrony Cyberprzestrzeni, w obszarze bezpieczeństwa informatycznego i teleinformatycznego.

2. Celami szczegółowymi Programu są:
   1) zwiększenie liczby kandydatów na studia wojskowe oraz cywilne z obszaru informatyki, kryptologii i cyberbezpieczeństwa posiadających odpowiednie przygotowanie informatyczne, z przeznaczeniem dla Sił Zbrojnych Rzeczypospolitej Polskiej i wyspecjalizowanych jednostek organizacyjnych resortu obrony narodowej;
   2) zapewnienie uczniom warunków do zdobywania wiedzy, umiejętności w obszarze współczesnych zagrożeń cyfrowych, zarządzania ryzykiem w sferze cyberbezpieczeństwa, bezpieczeństwa systemów informacyjnych, systemów bezpieczeństwa sieciowego oraz kryptograficznych aspektów ochrony danych, z przeznaczeniem do pracy w jednostkach organizacyjnych resortu obrony narodowej z zakresu cyberbezpieczeństwa;
   3) stworzenie uczniom warunków do rozwijania umiejętności i zdobywania wiedzy z zakresu zaawansowanej matematyki, informatyki i innych nauk wykorzystywanych w obszarze cyberbezpieczeństwa;
   4) stworzenie nauczycielom warunków do rozwijania umiejętności i zdobywania wiedzy z zakresu metodyki uczenia zaawansowanej matematyki, informatyki i innych nauk wykorzystywanych w obszarze cyberbezpieczeństwa.
3. Stanem oczekiwanym jest ochotnicze podejmowanie przez absolwentów oddziałów cyberbezpieczeństwo służby wojskowej w jednostkach organizacyjnych podległych Ministrowi Obrony Narodowej lub przez niego nadzorowanych, w tym w jednostkach podległych Narodowemu Centrum Bezpieczeństwa Cyberprzestrzeni, zwanemu dalej „NCBC", Eksperckim Centrum Szkolenia Cyberbezpieczeństwa, zwanemu dalej „ECSC", zatrudnienie w charakterze pracowników wojska w tych jednostkach lub kontynuacja nauki w Wojskowej Akademii Technicznej, zwanej dalej „WAT", Akademii Marynarki Wojennej, zwanej dalej „AMW", albo w innych uczelniach krajowych realizujących program ochotniczego szkolenia wojskowego studentów „Legia Akademicka" z zamiarem podjęcia służby wojskowej lub zatrudnienia w resorcie obrony narodowej.

Rozdział IV. Założenia organizacyjne i sposób realizacji Programu

1. Program przeznaczony jest dla uczniów szkół ponadpodstawowych (liceum lub technikum) pobierających naukę w oddziale cyberbezpieczeństwo.
2. Przystąpienie szkół do Programu jest dobrowolne.
3. Założeniem Programu jest utworzenie 16 oddziałów realizujących nauczanie w obszarze cyberbezpieczeństwa i nowoczesnych technologii informatycznych, średnio w jednej szkole na terenie każdego województwa, przy zastosowaniu innowacyjnych działań programowych, organizacyjnych lub metodycznych.
4. Jeżeli w danym województwie brakuje potencjału do utworzenia oddziału, możliwe jest utworzenie dwóch oddziałów w innym województwie, lub zmniejszenie liczby szkół uczestniczących w Programie.
5. Oddział cyberbezpieczeństwo powinien liczyć nie mniej niż 10 i nie więcej niż 15 uczniów.
6. Program nauczania przedmiotów specjalistycznych w oddziale cyberbezpieczeństwo realizuje się przez pierwsze 3 lata szkolne. Każdy rok nauki obejmuje 70 godzin lekcyjnych.

Nauka w ostatniej klasie stanowi przygotowanie do egzaminu maturalnego.

7. W ostatniej klasie nauki w ramach godzin z zajęć z doradztwa zawodowego uczniowie powinni odbyć minimum 3 godziny lekcyjne poświęcone przybliżeniu zawodu żołnierza.
8. W ramach Programu realizuje się następujące obszary tematyczne: podstawy kryptografii, historia kryptografii, podstawy algorytmiki, podstawy cyberbezpieczeństwa, zarządzanie bezpieczeństwem danych i informacji.
9. Nauka w oddziale objętym Programem umożliwi uczniom zdobycie wiedzy i kompetencji z obszaru współczesnych zagrożeń cyfrowych, zarządzania ryzykiem w zakresie cyberbezpieczeństwa, bezpieczeństwa systemów informacyjnych oraz kryptograficznych aspektów ochrony danych.
10. Absolwenci oddziałów cyberbezpieczeństwa będą mieli – po wdrożeniu przez Ministerstwo Obrony Narodowej, zwane dalej „MON", elementów motywacyjnych – większe szanse na przyjęcie na studia wojskowe z zakresu cyberbezpieczeństwa, informatyki i przedmiotów ścisłych.
11. Zgłoszenie szkoły do Programu jest równoznaczne z jego akceptacją.
12. Szkoła uczestnicząca w Programie jest zobowiązana do przestrzegania i stosowania jego reguł.
13. W razie nie wywiązywania się zakwalifikowanej szkoły z przyjętych zobowiązań, nie spełniania wymagań lub niewłaściwego wydatkowania środków budżetowych, Minister Obrony Narodowej może odstąpić od wsparcia szkoły, jak również zażądać zwrotu dotacji celowych.

Rozdział V. Uczestnicy Programu

Podmioty uczestniczące ze strony MON

1. Biuro do spraw Programu „Zostań Żołnierzem Rzeczypospolitej", zwane dalej „Biurem", odpowiada za:
   1) koordynację Programu, nadzór nad jego realizacją, sprawozdawczość oraz jego ewaluację;
   2) czynności prawne i faktyczne związane z umowami na przekazanie dotacji, na podstawie odrębnego pełnomocnictwa udzielonego dyrektorowi Biura przez Ministra Obrony Narodowej;
   3) obsługę organizacyjną Programu.
2. AMW obejmie patronat naukowy nad realizacją Programu.
3. NCBC sprawuje nadzór merytoryczny nad realizacją Programu. NCBC sporządza coroczną ocenę z realizacji programu kształcenia w szkołach uczestniczących w Programie.
4. NCBC, AMW, ECSC oraz WAT udzielają szkołom wsparcia w realizacji Programu oraz w miarę możliwości uczestniczą w realizacji programu kształcenia.
5. Departament Budżetowy odpowiada za obsługę finansowo-księgową Programu.
6. AMW opracuje program kształcenia przedmiotów specjalistycznych w oparciu o przygotowany przez WAT we współpracy z NCBC projekt ramowego planu kształcenia, w celu wykorzystania przez szkoły uczestniczące w Programie.
7. Ramowy plan kształcenia oraz program kształcenia przedmiotów specjalistycznych należy traktować jako pomoc niezbędną do opracowania przez właściwe szkoły własnych

programów nauczania realizowanych na terenie szkoły. W zależności od potrzeb program może być modyfikowany, tak żeby odpowiadał potrzebom zespołu uczniowskiego. Dopuszczalna jest także nieznaczna zmiana liczby godzin kształcenia specjalistycznego w cyklu realizacji Programu, podczas którego dany przedmiot jest realizowany. Zmiany nie mogą skutkować zagrożeniem realizacji celu głównego oraz celów szczegółowych Programu, o których mowa w rozdziale III.

8. Zajęcia dydaktyczne z podstaw kryptografii, podstaw cyberbezpieczeństwa, bezpiecznych infrastruktur informatycznych, historii kryptografii, podstaw algorytmiki i innych przedmiotów specjalistycznych mogą być prowadzone przez nauczycieli akademickich z dyscyplin w zakresie nauk technicznych, na zasadzie zawartych porozumień.
9. W ramach kształcenia przewidziane są zajęcia teoretyczne oraz laboratoryjne z wykorzystaniem nowoczesnych systemów operacyjnych i pakietów obliczeń symbolicznych. Dopuszcza się prowadzenie zajęć nauczania zdalnego (e-learning), organizowanie wizyt studyjnych i dydaktycznych w jednostkach organizacyjnych resortu obrony narodowej, instytutach naukowych oraz przedsiębiorstwach zajmujących się analizą, kontrolą i działaniami związanymi z cyberbezpieczeństwem.
10. Do prowadzenia zajęć specjalistycznych mogą być również wykorzystani specjaliści z podmiotów gospodarczych, w szczególności działających w branży informatycznej i zbrojeniowej, z zachowaniem zasad ochrony informacji niejawnych i zgodnie z przepisami dotyczącymi wsparcia szkół.
11. W procesie realizacji Programu przewiduje się również udział innych podmiotów: organów administracji państwowej, organów prowadzących szkoły, uczelni, komórek i jednostek organizacyjnych resortu obrony narodowej oraz zainteresowanych podmiotów gospodarczych, w zakresie oddelegowania ekspertów lub zorganizowania praktyk, konkursów lub obozów dla uczniów.

<u>Podmioty uczestniczące ze strony instytucji oświatowych</u>

1. Program skierowany jest do szkół ponadpodstawowych, które zostały wyłonione na podstawie zarządzenia Nr 12/MON Ministra Obrony Narodowej z dnia 23 kwietnia 2020 r. w sprawie wdrożenia „Programu CYBER.MIL z klasą" (Dz. Urz. Min. Obr. Nar. poz. 73).
2. Na etapie podpisania umowy na przekazanie dotacji celowej z organem prowadzącym szkołę, organ ten przedstawia dodatkowo:
   1) list intencyjny z uczelni wyższej, posiadającej w ofercie przedmioty z zakresu matematyki lub informatyki, lub z innego uprawnionego podmiotu o możliwości sprawowania opieki nad realizacją Programu;
   2) kalkulację kosztów (kosztorys) utworzenia oddziału cyberbezpieczeństwo;
   3) dokumenty świadczące o realizacji działalności dydaktyczno-wychowawczej w dziedzinie obronności państwa;
   4) oświadczenia dotyczące spełniania wymogów formalnych określonych w Programie oraz w przepisach prawa oświatowego wraz z kserokopiami dokumentów.

<u>Uczniowie</u>

1. Nabór do oddziału cyberbezpieczeństwo jest dobrowolny.
2. W postępowaniu rekrutacyjnym bierze się pod uwagę oceny z matematyki, informatyki, fizyki oraz z języka angielskiego.
3. Kandydaci przystępujący do rekrutacji muszą wykazać się uzyskaniem w procesie rekrutacji minimum 150 punktów oraz oceny co najmniej dobrej na świadectwie ukończenia szkoły

podstawowej z przedmiotów, o których mowa w pkt 2, a także powinni deklarować zainteresowanie problematyką obronności i wojska.

4. Ukończenie nauki w oddziale cyberbezpieczeństwo nie wiąże się z obowiązkiem podjęcia służby wojskowej lub zatrudnienia w resorcie obrony narodowej.
5. Nieukończenie nauki w oddziale cyberbezpieczeństwo nie wymaga zwrotu środków finansowych wydanych na cele związane z wyposażeniem i funkcjonowaniem pracowni informatycznych oraz wynagrodzeniem dla nauczycieli uczących przedmiotów specjalistycznych.

Rozdział VI. Okres realizacji Programu

1. Czas realizacji Programu określa się na okres 9 lat.
2. Program dzieli się na cykle nauczania, z których każdy trwa 4 lata.
3. Rekrutację uczniów do I klasy oddziału cyberbezpieczeństwo przeprowadza się przez okres pierwszych sześciu lat realizacji Programu.
4. Minister Obrony Narodowej potwierdza corocznie rekrutację, o której mowa w pkt 3.
5. Minister Obrony Narodowej może zakończyć realizowany w szkole Program po przeprowadzeniu jego częściowej ewaluacji lub braku środków finansowych przeznaczonych na ten cel.
6. Zakończenie Programu w szkole musi uwzględniać ukończenie przez uczniów oddziału cyberbezpieczeństwo 4-letniego cyklu nauczania.
7. Minister Obrony Narodowej może zezwolić na kontynuację Programu po dokonaniu jego ewaluacji w 9 roku realizacji Programu.

Rozdział VII. Przebieg realizacji Programu

1. Szkoły zakwalifikowane do Programu mogą ubiegać się o dotację celową na dofinansowanie realizacji Programu. Dotacja zostanie przekazana na podstawie umowy zawartej pomiędzy Skarbem Państwa – Ministrem Obrony Narodowej a organem prowadzącym szkołę.
2. Szkoły uczestniczące w Programie z otrzymanej dotacji celowej i środków własnych organu prowadzącego szkołę:
   1) przeprowadzą zakupy sprzętu, wyposażenia ucznia oraz inwestycje związane z urządzeniem pracowni komputerowych;
   2) zapewnią kadrę dydaktyczną, gwarantującą wysoki poziom nauczania oraz zorganizują współpracę z podmiotami zewnętrznymi określonymi w Programie.
3. MON może udzielić wsparcia merytorycznego szkołom biorącym udział w Programie, poprzez między innymi delegowanie ekspertów z zakresu cyberbezpieczeństwa z komórek i jednostek organizacyjnych resortu obrony narodowej.

Rozdział VIII. Zakres i tryb finansowania Programu

<u>Zasady finansowania Programu</u>

1. Program będzie dofinansowany ze środków publicznych, których dysponentem jest Minister Obrony Narodowej, w formie dotacji celowych.
2. Dotacje celowe udzielane są organom prowadzącym szkoły z oddziałami cyberbezpieczeństwa na podstawie ustawy z dnia 27 października 2017 r. o finansowaniu

zadań oświatowych oraz ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych.

3. W ramach dotacji celowych i środków własnych organów prowadzących szkoły zostaną zapewnione środki finansowe na cele związane z:
   1) wynagrodzeniem dla osób prowadzących zajęcia z przedmiotów specjalistycznych;
   2) zakupem wyposażenia ucznia;
   3) wyposażeniem i funkcjonowaniem pracowni informatycznych, w szczególności na zakup:
      a) sprzętu komputerowego, urządzeń towarzyszących (m.in. drukarki, tablicy interaktywnej, projektora multimedialnego) oraz urządzeń sieciowych wraz z montażem,
      b) dostępu do Internetu i dostarczanie usług internetowych,
      c) licencji i oprogramowania,
      d) mebli i wyposażenia do pomieszczeń przeznaczonych na pracownie informatyczne (m.in. klimatyzacja) wraz z montażem;
      e) specjalistycznej literatury branżowej.
4. Liczbę stanowisk komputerowych niezbędnych do realizacji Programu w oddziale cyberbezpieczeństwo określa się na równą maksymalnej liczbie uczniów, o której mowa w pkt 5 w rozdziale IV, powiększonej o dwa stanowiska dodatkowe – jedno stanowisko zapasowe i jedno dla nauczyciela.
5. Po zakończeniu cyklu nauczania Minister Obrony Narodowej na wniosek organu prowadzącego szkołę może udzielić ponownej dotacji, o której mowa w pkt 3 ppkt 3 lit. a i c, na zasadach określonych w pkt 4.
6. W uzasadnionych przypadkach na wniosek organu prowadzącego szkołę Minister Obrony Narodowej może udzielić dotacji, o której mowa w pkt 5, przed zakończeniem cyklu nauczania. Wniosek wymaga pozytywnej opinii NCBC.
7. Szczegółowe zasady dotyczące przyznania dotacji, ich rozliczania, kontroli i sprawozdawczości zostaną uregulowane w umowach.

Rozdział IX. Sposób oceny realizacji i ewaluacja Programu

1. Program podlega okresowej ewaluacji przez Biuro.
2. Przeprowadzenie pierwszej ewaluacji Programu nastąpi po upływie 3 lat od jego wprowadzenia, jednak nie później niż do zakończenia 4-letniego cyklu nauczania.
3. Pełna ewaluacja Programu nastąpi w ostatnim roku jego realizacji.
4. Szkoła uczestnicząca w Programie przesyła do Biura i NCBC sprawozdania zawierające informacje na temat procesu wdrożenia Programu oraz realizacji treści nauczania, po zakończeniu każdego cyklu nauczania przedmiotów specjalistycznych przez cały okres trwania Programu oraz w ostatnim roku realizacji Programu.
5. Na podstawie przesłanych sprawozdań Biuro dokonuje analizy i oceny efektywności i użyteczności wdrożenia Programu.
6. Do analizy, oceny i ewaluacji Programu zostanie włączone Wojskowe Centrum Edukacji Obywatelskiej w zakresie realizacji przez podległe mu Wojskowe Biuro Badań Społecznych okresowych badań ankietowych wśród wszystkich podmiotów zaangażowanych w jego realizację. Ankiety będą tworzone we współpracy z AMW.
7. Upoważnieni przedstawiciele Ministra Obrony Narodowej mogą prowadzić kontrolę

(nadzór) nad realizacją Programu.

8. Wnioski opracowane na podstawie sprawozdań będą udostępniane organom prowadzącym szkoły oraz dyrektorom szkół uczestniczących w Programie.
9. Dopuszcza się dokonanie w Programie niezbędnych, uzasadnionych zmian, po analizie wyników opracowanych na podstawie sprawozdań.