

INSTRUKCJA DLA UŻYTKOWNIKA PLATFORMY „SZKOLENIE OBRONNE”
uczestnika części teoretycznej wyższego kursu obronnego (dalej „kurs”)

Zapraszamy na platformę „szkolenie obronne”:

<https://szkolenieobronne.elearning.wp.mil.pl/login/index.php>.

Zaloguj do Platforma e-learning Szkolenia Obronnego

Zaloguj się

[Zapomniałeś hasła?](#)

Polski (pl) ▾

Powiadomienie o plikach cookie

Szkolenie odbywa się w formie asynchronicznego e-learningu, samodzielnie zapoznajesz się z przygotowanymi dla Ciebie materiałami.

1. Dostęp do Twojego kursu uzyskasz po zalogowaniu.
2. Login (nazwę użytkownika) i hasło otrzymasz po zweryfikowaniu Twojego zgłoszenia.
3. Po zalogowaniu na platformę, przed rozpoczęciem kursu musisz jednorazowo (czynności nie trzeba powtarzać przy kolejnych logowaniach):

☐ zmienić hasło

Aby kontynuować, musisz zmienić swoje hasło.

×

Zmień hasło

Nazwa użytkownika

tester

Hasło musi mieć co najmniej 8 znaków, cyfr co najmniej 1, co najmniej 1 małych liter, co najmniej 1 dużych liter, co najmniej 1 znaków niestandardowych (takich jak *, - lub #)

Obecne hasło

!

Nowe hasło

!

Nowe hasło (ponownie)

!

Zapisz zmiany

wymagane !

☐ zaakceptować PESO (regulamin funkcjonowania platformy szkoleniowej) oraz potwierdzić zapoznanie się z instrukcją dla użytkownika platformy „szkolenie obronne”

Potwierdź

Musisz zaakceptować te zasady, żeby używać strony. Czy zgadzasz się?



Dodatkowo uzyskujesz dostęp do fakultatywnej kategorii *Zagrożenia w cyberprzestrzeni i prewencja terrorystyczna*. Aby zapoznać się z materiałami skorzystaj z odrębnego loginu i hasła (otrzymujesz go w tym samym mailu).

Następne logowanie:

Ze względów bezpieczeństwa na platformie szkolenia obronnego obowiązuje dwuskładnikowy proces logowania MFA (ang. *Multi-Factor Authentication*).

Ważne informacje:

- do skonfigurowania MFA konieczny jest smartfon z poprawnie działającą kamerą (aparatem);
- konfigurowania MFA jest proste i intuicyjne;
- przy każdym logowaniu na platformie, poza loginem i hasłem, trzeba wpisać kod generowany przez aplikację Authenticator;
- aplikacja Authenticator generuje kod co 30 sekund, jest to czas na wpisanie go w okno na platformie (jeśli minie 30 sekund i kod nie zostanie wpisany – traci on ważność i jest generowany nowy kod do wpisania);
- w przypadku problemów z konfiguracją aplikacji Authenticator lub wprowadzeniem kodu (kod zostaje odrzucony – komunikat „błędny kod”) należy skontaktować się z lokalnym administratorem sieci lub informatykiem odpowiadającym w danej instytucji za administrowanie siecią;
- limit błędnych kodów z aplikacji Authenticator wynosi 10, po jego przekroczeniu możliwość zalogowania się na platformę zostanie zablokowana. Konto może odblokować jedynie administrator platformy.

Instrukcja Logowania z MFA

1. Pierwsze logowanie po wdrożeniu MFA:
 - zaloguj się na platformę tak jak dotychczas, używając swojego loginu i hasła;
 - po wprowadzeniu poprawnych danych logowania, zostaniesz poproszony o skonfigurowanie aplikacji typu Authenticator. W tym celu należy postępować zgodnie z poniższymi krokami:
- Pobranie aplikacji Authenticator:
 - pobierz i zainstaluj aplikację Authenticator na swoim urządzeniu mobilnym (np. **Microsoft Authenticator**, **Google Authenticator**).



Google
Authenticator

- Rekomendowane przez nas aplikacje są **BEZPŁATNE**.

Musisz zakończyć konfigurację uwierzytelniania wieloskładnikowego, zanim będziesz mógł kontynuować.

Dostępne składniki

Aplikacja Authenticator

Użyj dowolnej aplikacji uwierzytelniającej TOTP, aby uzyskać kod weryfikacyjny na telefonie, nawet jeśli jest on offline.

np.

- [Twilio Authy](#)
- [Microsoft Authenticator](#)
- Google Authenticator dla [iOS](#) czy [Android](#)

Uwaga: Upewnij się, że czas i data urządzenia zostały ustawione na "Auto" lub "Sieć dostarczona".

Ustaw aplikację

- Konfiguracja aplikacji:
 - zaloguj się na platformie
 - wybierz opcję konfiguracji MFA i wybierz metodę Authenticator.
 - wyświetlony kod QR, należy zeskanować za pomocą aplikacji Authenticator.
 - hasło jednorazowe

Konfiguracja uwierzytelniacza TOTP

Użyj dowolnej aplikacji uwierzytelniającej TOTP, aby uzyskać kod weryfikacyjny na telefonie, nawet jeśli jest on offline.

np.

- [Twilio Authy](#)
- [Microsoft Authenticator](#)
- [Google Authenticator dla iOS czy Android](#)

Uwaga: Upewnij się, że czas i data urządzenia zostały ustawione na "Auto" lub "Sieć dostarczona".

Etykieta urządzenia

Szkolenie obronne

Zeskanuj kod QR:

Zeskanuj kod QR za pomocą wybranej aplikacji uwierzytelniania.



LUB otwórz aplikację mobilną:

Otwórz aplikację już zainstalowaną na tym urządzeniu

Nie możesz zeskanować?

Wprowadź kod weryfikacyjny w celu potwierdzenia

Zapisz zmiany

Anuluj

wymagane

- Skanowanie kodu QR:
 - otwórz aplikację Authenticator na swoim urządzeniu mobilnym i zeskanuj kod QR wyświetlony na platformie.
- Wprowadzenie kodu:
 - aplikacja Authenticator wygeneruje sześciocyfrowy kod. Wprowadź ten kod na platformie, aby zakończyć konfigurację.
- Potwierdzenie:
 - po wprowadzeniu poprawnego kodu, aplikacja Authenticator będzie skonfigurowana jako metoda uwierzytelniania. Od tej pory, przy każdym logowaniu będziesz używać kodu generowanego przez aplikację Authenticator.

Aplikacja Authenticator

Wprowadź kod weryfikacyjny w celu potwierdzenia

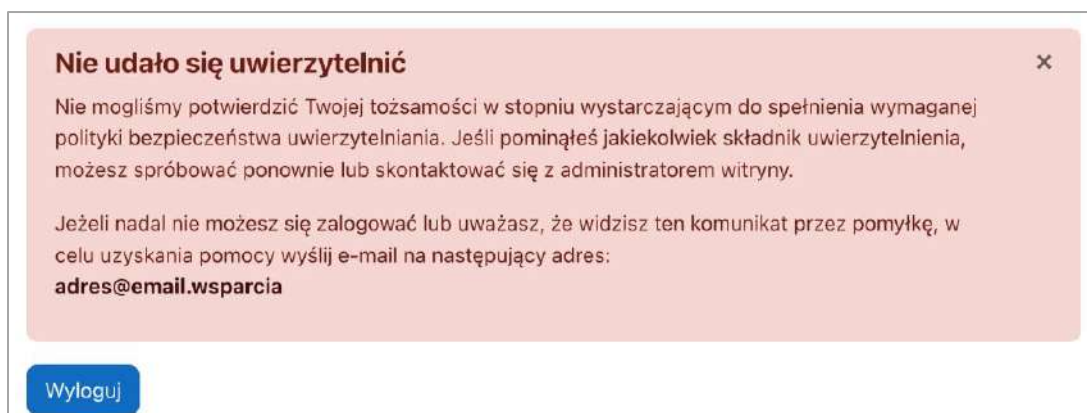
Zweryfikuj kod

Nie mam swojego urządzenia

2. Po weryfikacji zostaniesz przeniesiony do strony głównej platformy.

Przerwanie procedury logowania:

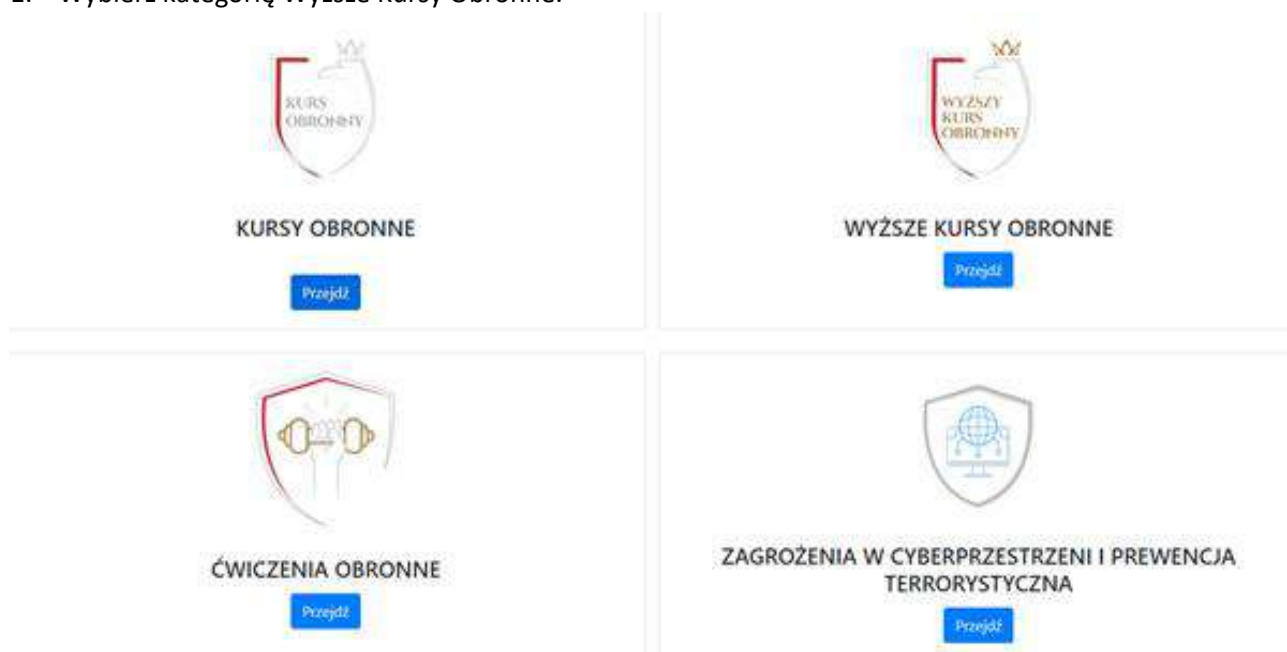
W sytuacji, kiedy przerwiesz procedurę logowania lub nie spełnisz warunków logowania MFA, przed wylogowaniem zobaczysz komunikat z informacją:



W przypadku zgubienia/zniszczenia telefonu, na którym użytkownik posiadał skonfigurowaną aplikację typu Authenticator, należy zgłosić ten fakt Menadżerowi Platformy.

Rozpocznij realizację kursu

1. Wybierz kategorię Wyższe Kursy Obronne.



UWAGA! otrzymujesz dostęp wyłącznie do zasobów swojej grupy (pozostałe zasoby są dla Ciebie niewidoczne).

2. Twój kurs składa się z zagadnień oraz tematów w ramach każdego z nich. Tematy są podzielone na obowiązkowe i fakultatywne.
3. Aby ukończyć kurs musisz zaliczyć wszystkie dedykowane Twojej grupie zagadnienia, a w ramach każdego zagadnienia – zapoznać się ze wszystkimi obowiązkowymi tematami (w postaci filmu lub prezentacji). **UWAGA!** Pełny wykaz zagadnień znajdziesz w pliku *podział na grupy szkoleniowe i przypisane im nr zagadnień* na stronie <https://www.gov.pl/web/obrona-narodowa/szkolenie-obronne>.

UWAGA! Jeśli wykład nie będzie chciał się uruchomić, musisz zezwolić na wyskakujące okna w swojej przeglądarce internetowej:

- w przeglądarce **Mozilla Firefox**, pod paskiem wpisywania strony internetowej, gdy pojawi się napis „Firefox uniemożliwił tej witrynie otwarcie wyskakującego okna”, należy kliknąć „Opcje” i wybrać „Pozwól ...”. Następnie należy odświeżyć stronę i wykład się uruchomi;
- w **innych przeglądarkach**, w pasku wpisywania strony internetowej, po prawej stronie pojawi się prostokąt z czerwonym iksem. Należy kliknąć na niego, zaznaczyć „Zawsze zezwalaj...” i nacisnąć „Gotowe”. Następnie należy odświeżyć stronę i wykład się uruchomi.

4. Aby otworzyć zagadnienie kliknij w jego tytuł.

ZAGROŻENIA BEZPIECZEŃSTWA NARODOWEGO

5. Zagadnienia możesz wybierać w dowolnej kolejności.
6. Nie musisz ukończyć zagadnienia (zaliczyć wszystkich tematów), aby przejść do innego zagadnienia. Jednak aby ostatecznie ukończyć kurs wszystkie zagadnienia musisz ukończyć/zaliczyć.

Tematy obowiązkowe: 1, 2
Tematy fakultatywne: 3, 4, 5

W tym miejscu zostały wypisane tematy obowiązkowe i fakultatywne

1. Istota i cele zarządzania kryzysowego. Rodzaje sytuacji kryzysowych - wykład z prezentacją	✓ Wykonano: Ukończ aktywność
2. Procedury zarządzania kryzysowego - wykład z prezentacją	✓ Wykonano: Ukończ aktywność
3. Zarządzanie komunikacją podczas kryzysu - wykład	Do wykonania: Ukończ aktywność
4. System zarządzania kryzysowego NATO (NCRS). Przełożenie na wymiar krajowy - wykład z prezentacją	Do wykonania: Ukończ aktywność

Zielone pole oznacza, że materiał został zaliczony.

Szare pole oznacza, że materiał nie został ukończony. tematu obowiązkowego musisz się z nim zapoznać (musi pojawić się zielone pole). W przypadku tematu fakultatywnego możesz go pominąć.

7. Ukończenie tematu powoduje powrót do strony zagadnienia (w ciągu kilku/kilkunastu sekund).

8. Zagadnienie 15 *Urząd w działaniu* pozwoli Ci zweryfikować zdobytą wiedzę. Nie jest to test zaliczeniowy, lecz forma quizu – praktycznego ćwiczenia. Zagadnienie nie jest obowiązkowe, można je pominąć lub zrealizować częściowo. Po zakończeniu zagadnienia wyświetlą się prawidłowe odpowiedzi.
9. Kurs kończy się jednym sprawdzianem wiedzy – testem jednokrotnego wyboru. Nie ma limitu podejść do testu. Pytania testowe są każdorazowo losowo wybierane przez system (zestaw pytań jest inny przy każdym podejściu do testu).
Test pojawi się dopiero gdy wszystkie zagadnienia zostaną ukończone. Aby do niego przejść należy kliknąć „Test wiedzy” w menu po lewej.

✓ Wykonano: Wyświetl

Do wykonania: Otrzymaj ocenę

Do wykonania: Otrzymaj ocenę pozytywną

Przed Tobą test składający się z 10 pytań.
Aby go zaliczyć należy prawidłowo odpowiedzieć na **co najmniej 6 pytań**.

Podgląd testu

Metoda oceniania: Najwyższa ocena

Próg zaliczeniowy: 6,00 na 10,00

10. Po zaliczeniu kursu kolejnym krokiem jest wypełnienie ankiety oceny kursu (obowiązkowe).
Aby przejść do ankiety kliknij „Sekcja ogólna” (w menu po lewej stronie na górze).

> Sekcja ogólna

> Informacje wstępne

> Test wiedzy

> REGULACJE PRAWNE BE...

> ORGANIZACJA LEKCYJ...

Wyższy Kurs Obronny

KursUczestnicyOcenyBaza pytań

Sekcja ogólna

11. Po zakończeniu kursu otrzymasz z platformy komunikat o treści jak poniżej.

GRATULACJE!

Ukończyłeś część teoretyczną Wyższego Kursu Obronnego.

12. Po zakończeniu kursu masz możliwość pobrania kompendium wiedzy w formacie PDF – podsumowania najbardziej istotnych informacji w ramach zagadnień dedykowanych Twojej grupie.



Jeśli masz pytania dotyczące funkcjonowania platformy i udziału w kursie:

- napisz na adres szkolenie.obronne@ron.mil.pl
lub
- zadzwoń (pomoc uzyskasz w godzinach 10.00-14.00 od poniedziałku do piątku z wyłączeniem dni wolnych od pracy):
 - 261 814 476
 - 261 814 433
 - 261 813 990
 - 261 813 449