Możliwość dofinansowania

CYB-101 Cyberbezpieczeństwo - praktyczne fundamenty (Cybersecurity Foundation) - szkolenie

Numer usługi 2026/07/29/18395/3717067

2 900,00 PLN brutto
2 900,00 PLN netto
138,10 PLN brutto/h
138,10 PLN netto/h
261,33 PLN cena rynkowa

Akademia Górniczo-Hutnicza im. Stanisława Staszica w Krakowie

4,6 / 5

45 ocen

Kraków
Usługa szkoleniowa
stacjonarna
Zajęcia grupowe
21:00 h
07.09.2026 do 09.09.2026

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Grupa docelowa usługi	Adresaci szkolenia to: pracownicy działów IT (helpdesk, wsparcie), nowi członkowie zespołów bezpieczeństwa, kadra zarządzająca średniego szczebla, liderzy projektów i procesów biznesowych, specjaliści ds. ryzyka oraz osoby z sektora komercyjnego, które chcą rozpocząć pracę w obszarze cyberbezpieczeństwa lub współpracują z działami security.
Minimalna liczba uczestników	8
Maksymalna liczba uczestników	16
Data zakończenia rekrutacji	03-09-2026
Forma prowadzenia usługi	stacjonarna
Podstawa uzyskania wpisu do BUR	art. 163 ust. 1 ustawy z dnia 20 lipca 2018 r. Prawo o szkolnictwie wyższym i nauce (t. j. Dz. U. z 2024 r. poz. 1571, z późn. zm.)
Zakres uprawnień	kształcenie w innych formachkształcenia prowadzonych przez uczelnie

Cel

Cel edukacyjny

Celem szkolenia jest wprowadzenie uczestników w praktyczne i biznesowe podstawy cyberbezpieczeństwa. Szkolenie porządkuje najważniejsze pojęcia, modele i mechanizmy bezpieczeństwa, oraz pokazuje krajobraz zagrożeń, z którym

mierzą się współczesne organizacje. Uczestnicy poznają m.in. zasady działania ataków socjotechnicznych, malware i ransomware, podstawy ochrony tożsamości, model Zero Trust, elementy reagowania na incydenty oraz najważniejsze ramy regulacyjne i standardy.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Charakteryzuje fundamentalne modele bezpieczeństwa informacji oraz krajobraz zagrożeń cybernetycznych	omawia triadę CIA i model AAA w kontekście celów biznesowych i ciągłości działania, rozróżnia typy atakujących i ich motywacje, analizuje wybrany głośny incydent pod kątem przyczyn i skutków biznesowych	Test teoretyczny
Rozpoznaje techniki inżynierii społecznej i ocenia wiarygodność podejrzanych komunikatów	identyfikuje mechanizmy phishingu, spear-phishingu, vishingu i baitingu w przykładowych scenariuszach, wskazuje ślady umożliwiające profilowanie pracowników w mediach społecznościowych (OSINT), ocenia wiarygodność wskazanej wiadomości/komunikatu i uzasadnia swoją ocenę	Test teoretyczny
Opisuje architekturę bezpieczeństwa IT, mechanizmy kryptograficzne oraz zasady zarządzania tożsamością i dostępem	charakteryzuje powierzchnię ataku sieci, endpointów i chmury, rozróżnia szyfrowanie symetryczne i asymetryczne oraz rolę certyfikatów SSL/TLS, uzasadnia zastosowanie MFA, modelu Zero Trust i zasady najmniejszych uprawnień w procesach biznesowych	Test teoretyczny
Rozróżnia rodzaje złośliwego oprogramowania i charakteryzuje przebieg ataku ransomware	klasyfikuje wirusy, trojany i oprogramowanie szpiegujące wg mechanizmu działania, opisuje kolejne etapy ataku ransomware od infekcji do żądania okupu, wskazuje biznesowe konsekwencje wybranego scenariusza ataku ransomware	Test teoretyczny
Planuje podstawowe działania w zakresie reagowania na incydenty oraz uwzględnia wymagania regulacyjne i kulturę bezpieczeństwa w codziennej pracy	opisuje kolejne fazy cyklu obsługi incydentu (przygotowanie, detekcja, ograniczenie, usunięcie, wnioski), rozróżnia zakres i cel ISO 27001, NIST CSF, RODO, DORA i NIS2.	Test teoretyczny

Kwalifikacje

Kompetencje

Usługa prowadzi do nabycia kompetencji.

Warunki uznania kompetencji

Pytanie 1. Czy dokument potwierdzający uzyskanie kompetencji lub wyraźnie z nim powiązane inne dokumenty związane ze wsparciem zawierają opis efektów uczenia się?

TAK

Pytanie 2. Czy dokument lub wyraźnie z nim powiązane inne dokumenty związane ze wsparciem potwierdzają, że walidacja została przeprowadzona w oparciu o zdefiniowane w efektach uczenia się kryteria ich weryfikacji i zgodnie z zaplanowanymi metodami walidacji?

TAK

Pytanie 3. Czy dokument lub wyraźnie z nim powiązane inne dokumenty związane ze wsparciem potwierdzają zastosowanie rozwiązań zapewniających rozdzielenie procesów kształcenia i szkolenia od walidacji?

TAK

Program

1. Fundamenty cyberbezpieczeństwa: triada CIA, model AAA, rola cyberbezpieczeństwa w zapewnieniu ciągłości działania.

2. Krajobraz zagrożeń: cyberprzestępczość jako usługa, profile atakujących, analiza incydentów.

3. Czynnik ludzki i inżynieria społeczna: phishing, spear-phishing, vishing, baiting, podstawy OSINT oraz warsztat identyfikacji ataków socjotechnicznych.

4. Bezpieczeństwo IT w pigułce: sieci, endpointy, chmura, powierzchnia ataku, kryptografia i przykłady ataków na aplikacje webowe.

5. Tożsamość i uprawnienia: hasła, MFA, biometria, Zero Trust, zasada najmniejszych uprawnień.

6. Malware i ransomware: rodzaje złośliwego oprogramowania, anatomia ataku, pokaz kontrolowanej infekcji.

7. Reagowanie na incydenty: cykl obsługi incydentu, rola pracowników, koszty biznesowe incydentów, rola zespołów bezpieczeństwa.

8. Ramy regulacyjne i standardy: wprowadzenie do ISO 27001, NIST CSF, RODO, DORA i NIS2 oraz bezpieczeństwo łańcucha dostaw.

9. Budowanie kultury bezpieczeństwa: security awareness i przełożenie zasad bezpieczeństwa na codzienną praktykę.

10. Cyberbezpieczeństwo w moim dziale: case study, podsumowanie i ścieżki dalszego rozwoju.

Zajęcia odbywają się w jednej grupie szkoleniowej. Na jednego uczestnika przypada jedno stanowisko komputerowe wraz z niezbędnym sprzętem i oprogramowaniem.

Walidacja będzie realizowana na ostatnich zajęciach w postaci testu teoretycznego.

Zgodnie z proporcją 60/40% przyjętą w programie szkolenia zajęcia obejmują ok. 14 godzin dydaktycznych (ok. 10,5 godziny zegarowej) części teoretycznej (wykład ekspercki) oraz ok. 10 godzin dydaktycznych (ok. 7,5 godziny zegarowej) części praktycznej (warsztaty, analizy przypadków, pokazy ataków).

Szkolenie realizowane jest stacjonarnie z jednogodzinną przerwą każdego dnia zajęć oraz 30-minutowym testem teoretycznym kończącym.

Harmonogram

Liczba pozycji harmonogramu: 14

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 14 Moduł 1: Wprowadzenie i Modele Bezpieczeństwa – triada CIA, model AAA, rola cyberbezpieczeństwa w zapewnieniu ciągłości działania (BCP). Wykład ekspercki.	Zajęcia	mgr inż. Tomasz Nal	07-09-2026	08:00	09:30	01:30
2 z 14 Moduł 2: Ewolucja Krajobrazu Zagrożeń – cyberprzestępczość jako usługa, profile atakujących, analiza głośnych incydentów. Wykład ekspercki, dyskusja moderowana.	Zajęcia	mgr inż. Tomasz Nal	07-09-2026	09:30	11:45	02:15
3 z 14 -	Przerwa	-	07-09-2026	11:45	12:45	01:00
4 z 14 Moduł 3: Czynnik Ludzki i Inżynieria Społeczna – phishing, spear-phishing, vishing, baiting, podstawy OSINT. Wykład, warsztat identyfikacji ataków socjotechnicznych.	Zajęcia	mgr inż. Tomasz Nal	07-09-2026	12:45	15:00	02:15

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
5 z 14 Moduł 4: Bezpieczeństwo IT w pigułce – sieci, endpointy, chmura, powierzchnia ataku, kryptografia dla nie-inżynierów. Wykład, pokaz (demo) atakowania aplikacji webowych.	Zajęcia	mgr inż. Tomasz Nal	08-09-2026	08:00	10:15	02:15
6 z 14 Moduł 5: Tożsamość, Uprawnienia i Granice Zaufania – hasła, MFA, biometria, Zero Trust, zasada najmniejszych uprawnień. Wykład ekspercki.	Zajęcia	mgr inż. Tomasz Nal	08-09-2026	10:15	11:45	01:30
7 z 14 -	Przerwa	-	08-09-2026	11:45	12:45	01:00
8 z 14 Moduł 6: Malware i Ransomware – rodzaje złośliwego oprogramowania, anatomia ataku ransomware. Wykład, pokaz (demo) kontrolowanej infekcji i szyfrowania stacji roboczej.	Zajęcia	mgr inż. Tomasz Nal	08-09-2026	12:45	15:00	02:15

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
9 z 14 Moduł 7: Reagowanie na incydenty – cykl obsługi incydentu, rola pracowników, koszty biznesowe incydentów, rola zespołów bezpieczeństwa. Wykład ekspercki, dyskusja moderowana.	Zajęcia	mgr inż. Tomasz Nal	09-09-2026	08:00	10:15	02:15
10 z 14 Moduł 8: Ramy Regulacyjne i Standardy – ISO 27001, NIST CSF, RODO, DORA, wprowadzenie do NIS2, bezpieczeństwo łańcucha dostaw. Wykład ekspercki.	Zajęcia	mgr inż. Tomasz Nal	09-09-2026	10:15	11:45	01:30
11 z 14 -	Przerwa	-	09-09-2026	11:45	12:45	01:00
12 z 14 Moduł 9: Budowanie „Human Firewall” – kultura bezpieczeństwa, przejście od polityk na papierze do codziennych nawyków. Wykład ekspercki.	Zajęcia	mgr inż. Tomasz Nal	09-09-2026	12:45	13:30	00:45

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
13 z 14 Moduł 10: Cyberbezpieczeństwo w moim dziale – case study, podsumowanie, Q&A i ścieżki dalszego rozwoju.	Zajęcia	mgr inż. Tomasz Nal	09-09-2026	13:30	14:30	01:00
14 z 14 -	Walidacja	-	09-09-2026	14:30	15:00	00:30

Podsumowanie

Rodzaj godzin	Liczba godzin
Suma godzin zegarowych usługi	21:00
w tym suma godzin zajęć	17:30
w tym suma godzin walidacji	00:30
w tym suma przerw	03:00
Suma godzin dydaktycznych bez przerw	24:00

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	2 900,00 PLN
Podmiot uprawniony do zwolnienia z VAT na podstawie art. 43 ust. 1 ustawy o VAT	
Koszt przypadający na 1 uczestnika netto	2 900,00 PLN
Koszt osobogodziny brutto	138,10 PLN
Koszt osobogodziny netto	138,10 PLN

Liczba godzin usługi

Rodzaj godzin	Liczba godzin
Liczba godzin zegarowych usługi	21:00

Prowadzący

Liczba prowadzących: 1

1 z 1

mgr inż. Tomasz Nal

Specjalista ds. cyberbezpieczeństwa w Centrum Bezpieczeństwa Informacji AGH. Praktyk z doświadczeniem w bezpieczeństwie aplikacji webowych, testach penetracyjnych oraz zarządzaniu podatnościami. W swojej pracy łączy perspektywę techniczną i biznesową, koncentrując się na realnych zagrożeniach, projektowaniu bezpiecznych procesów oraz świadomym zarządzaniu ryzykiem. Posiada doświadczenie w prowadzeniu szkoleń dla sektora publicznego.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Uczestnicy otrzymają materiały bezpośrednio związane z realizowaną usługą oraz dokument potwierdzający udział/ukończenie szkolenia po zdaniu testu teoretycznego.

Adres

ul. Władysława Reymonta 23/D-8
30-055 Kraków
woj. małopolskie

Udogodnienia w miejscu realizacji usługi

- Klimatyzacja
- Wi-fi
- Laboratorium komputerowe

Kontakt

Agata Rzepka

E-mail szkolenia@informatyka.agh.edu.pl
Telefon (+48) 12 3283 414