Program studiów

Kierunek: Zarządzanie zintegrowanym bezpieczeństwem przedsiębiorstwa

Spis treści

Program studiów podyplomowych 3
Efekty uczenia się 6

Opis studiów podyplomowych

Ogólne informacje o studiach podyplomowych

Wydział:	Wydział Informatyki
Nazwa studiów podyplomowych (w j. polskim):	Zarządzanie zintegrowanym bezpieczeństwem przedsiębiorstwa
Nazwa studiów podyplomowych (w j. angielskim):	Integrated Enterprise Security Management
Poziom:	Studia podyplomowe
Termin rozpoczęcia cyklu:	2026/2027, semestr zimowy
Czas trwania jednej edycji studiów podyplomowych (liczba semestrów):	2
Język wykładowy:	polski
Liczba punktów ECTS wymagana do ukończenia studiów podyplomowych:	30
w tym: liczba punktów ECTS przypisanych do zajęć kształtujących umiejętności praktyczne:	12
w tym: liczba punktów ECTS przypisanych do zajęć prowadzonych z wykorzystaniem metod i technik kształcenia na odległość:	13

Data planowanego rozpoczęcia i zakończenia pierwszej edycji studiów podyplomowych

1 października 2026 - 30 września 2027

Zakres tematyczny

Studia podyplomowe „Zarządzanie zintegrowanym bezpieczeństwem przedsiębiorstwa" to kompleksowy, praktyczny program, który odpowiada na rosnące wyzwania współczesnych organizacji w zakresie bezpieczeństwa.
Wobec dynamicznego rozwoju zagrożeń hybrydowych, cyberataków, przestępczości gospodarczej, szpiegostwa korporacyjnego oraz zaostrzonych wymogów prawnych (m.in. dyrektywy NIS2 i DORA, zmiany w prawie BHP), przedsiębiorstwa potrzebują specjalistów posiadających holistyczne kompetencje, a nie tylko wąską specjalizację. Program wypełnia tę lukę na rynku, integrując w spójną całość kluczowe obszary bezpieczeństwa organizacji.
Program łączy wiedzę i umiejętności z zakresu:
- prawa i regulacji,
- zarządzania ryzykiem,
- cyberbezpieczeństwa i ochrony informacji,
- przeciwdziałania fraudom i szpiegostwu korporacyjnemu,
- ochrony fizycznej i technicznej,
- ciągłości działania i zarządzania kryzysowego,
- analizy informacji biznesowej,
- zarządzania zasobami ludzkimi w kontekście bezpieczeństwa.

Zajęcia mają charakter praktyczny – realizowane są w formie warsztatów, symulacji incydentów, analizy rzeczywistych przypadków oraz projektowania rozwiązań wdrożeniowych.

Do kogo adresowane są studia podyplomowe

Studia skierowane są do kadry zarządzającej wyższego i średniego szczebla oraz ekspertów pełniących kluczowe funkcje decyzyjne w organizacjach biznesowych i administracji publicznej. Zapraszamy dyrektorów departamentów, menedżerów ds. ryzyka, audytorów, którzy na co dzień odpowiadają za strategiczną ochronę informacji i zapewnienie ciągłości działania. To również przestrzeń dla ambitnych profesjonalistów z potencjałem liderskim, przygotowujących się do awansu i chcących zdobyć zaawansowane instrumentarium niezbędne do budowania kompleksowej odporności nowoczesnych instytucji.

Kierownik studiów podyplomowych: dr Krzysztof Krassowski
tel.: 12 617 43 39
mail: kkr@agh.edu.pl

Organizator studiów podyplomowych: Wydział Informatyki
tel.: 12 32 83 400
mail: informatyka@agh.edu.pl

Osoba do kontaktu: mgr Agata Rzepka
tel.: 12 32 83 414
mail: rzepka@agh.edu.pl

Dodatkowe informacje

Warunki rekrutacji na studia podyplomowe

Uczestnikami studów mogą być osoby posiadające wykształcenie wyższe, pragnące rozpocząć swoją pracę lub pogłębić posiadane kwalifikacje w zakresie zarządzania wszelkimi aspektami bezpieczeństwa przedsiębiorstwa, czy szerzej organizacji. Uczestnik powinien ponadto legitymować się podstawowymi kwalifikacjami w zakresie pracy z komputerem, zasobami internetowymi, dokumentami oraz danymi.

Program studiów podyplomowych

Ogólne cele kształcenia w ramach studiów podyplomowych

Celem kształcenia jest wyposażenie uczestników w praktyczne umiejętności identyfikacji zagrożeń, analizy ryzyka i projektowania zintegrowanych systemów bezpieczeństwa, przygotowanie do reagowania na incydenty, zarządzania kryzysowego oraz wdrażania norm ISO i przepisów prawa, rozwój kompetencji w zakresie analizy informacji biznesowej, zarządzania personelem struktur bezpieczeństwa, bezpiecznej rekrutacji i komunikacji wewnętrznej.

Sylwetka absolwenta studiów podyplomowych

Absolwent posiada praktyczne kompetencje do identyfikacji, analizy i zarządzania zintegrowanym bezpieczeństwem organizacji (BHP + cyber + informacje + fizyczne + kryzysowe + HR). Potrafi oceniać ryzyka na poziomie operacyjnym i strategicznym, projektować i wdrażać elementy systemów zarządzania (ISO 45001, 27001, 22301, NIS2/DORA), reagować na incydenty (cyber, fraud, wyciek, włamanie), przeprowadzać analizy informacji o kontrahentach (KYC analityczne, OSINT) oraz integrować procesy HR z bezpieczeństwem (bezpieczna rekrutacja, zarządzanie konfliktami, off-boarding, komunikacja wewnętrzna).

Jest przygotowany do roli specjalisty/menedżera ds. bezpieczeństwa organizacji, koordynatora compliance/ryzyka lub członka zespołu kryzysowego w średnich i dużych przedsiębiorstwach.

Zasady odbywania studiów podyplomowych, w tym zasady udziału w zajęciach, zasady zaliczania zajęć i zasady składania egzaminów, zasady zaliczania i wpisu na kolejny semestr

Do zaliczenia przedmiotów wymagana jest obecność na zajęciach oraz aktywny w nich udział. Przedmioty, w ramach których prowadzi się zajęcia w formie ćwiczeń i warsztatów kończą się zaliczeniem na ocenę (zwykle wystawianą na podstawie samodzielnie zrealizowanych i indywidualnie ocenianych zadań), która potem stanowi część oceny końcowej.

Wymiar, zasady , forma i miejsce odbywania praktyk, w tym w szczególności warunki ich realizacji, system kontroli praktyk i ich zaliczania (jeżeli są wymagane)

Nie dotyczy.

Warunki ukończenia studiów podyplomowych i uzyskania świadectwa ukończenia studiów podyplomowych, w tym warunki i wymagania związane z przygotowaniem prac końcowych oraz realizacją procesu dyplomowania, a także związane z organizacją i przebiegiem egzaminu końcowego (jego zakres, tryb i sposób jego przeprowadzenia, zasady ustalania oceny z egzaminu końcowego, wytyczne dotyczące jego przebiegu), jeżeli są wymagane, zasady ustalania ostatecznego wyniku ich ukończenia

Ocena końcowa uzyskiwana przez absolwentów studiów jest zgodna z przepisami Regulaminu studiów podyplomowych w AGH. Wymagane jest zaliczenie wszystkich przedmiotów. Ocena końcowa tworzona jest w oparciu o średnią ważoną z ocen uzyskanych z poszczególnych przedmiotów. Szczegółowy tryb zaliczenia jest ustalany indywidualnie dla każdego przedmiotu i podawany na pierwszych zajęciach z danego przedmiotu. W przypadku nieobecności należy uzgodnić z prowadzącym tryb odrobienia zaległości.

Informacja o możliwości odbycia kształcenia przygotowującego do wykonywania zawodu lub uzyskania uprawnień zawodowych w ramach nowo tworzonych studiów podyplomowych (o ile dotyczy)

Nie dotyczy.

Informacja o możliwości odbycia kształcenia zgodnie ze standardem kształcenia przygotowującego do wykonywania zawodu nauczyciela (o ile dotyczy)

Nie dotyczy.

Informacja o możliwości uzyskania przygotowania do wykonywania zawodu nauczyciela wraz ze wskazaniem przedmiotu lub rodzaju zajęć, które absolwent będzie mógł prowadzić po ukończeniu studiów podyplomowych (o ile dotyczy)

Nie dotyczy.

Efekty uczenia się

Kierunek: Zarządzanie zintegrowanym bezpieczeństwem przedsiębiorstwa

Wiedza

Symbol KEU	Kierunkowe efekty uczenia się	Symbol CEU
ZZBPSP_W01	Zna aktualne regulacje prawne i normatywne: Kodeks pracy i zmiany BHP (w tym czynniki psychospołeczne), RODO, NIS2, DORA, AI Act, ustawa o ochronie osób i mienia, AML/CFT, sygnaliści, MAR, art. 296 k.k. i odpowiedzialność podmiotów zbiorowych	P6S_WK
ZZBPSP_W02	Rozumie mechanizmy i trendy zagrożeń: fraudy wewnętrzne i zewnętrzne (BEC + deepfake), ransomware RaaS, ataki na łańcuch dostaw, insider threat, szpiegostwo korporacyjne (hybrydowe), dezinformacja biznesowa, zagrożenia fizyczne (włamania, sabotaż)	P6S_WG
ZZBPSP_W03	Zna metody analizy i weryfikacji informacji: krytyczne myślenie, KYC analityczne, OSINT (triangulacja, grafy powiązań), analiza hipotez konkurencyjnych (ACH), raportowanie z oceną pewności	P6S_WK
ZZBPSP_W04	Zna i rozumie zasady systemów zarządzania bezpieczeństwem: ISO 45001, ISO 27001, ISO 22301, ISO 31000 oraz ich praktyczne mapowanie na NIS2 i DORA	P6S_WG
ZZBPSP_W05	Zna procesy reagowania na incydenty: cykl NIST/SANS/ENISA, obowiązki raportowe (PUODO 72 h, CSIRT 24 h, KNF/DORA), komunikacja kryzysowa	P6S_WK
ZZBPSP_W06	Zna metody i narzędzia, w tym techniki pozyskiwania danych, właściwe dla dziedzin i dyscyplin naukowych przypisanych dla kierunku studiów, pozwalające opisywać struktury, powiązania oraz procesy w nich i pomiędzy nimi zachodzące	P6S_WK
ZZBPSP_W07	Zna funkcjonowanue ochrony fizycznej i technicznej: strefowanie obiektu, systemy kontroli dostępu (KD/ACS), monitoring wizyjny (CCTV + RODO), SSWiN, zabezpieczenia obwodowe	P6S_WK
ZZBPSP_W08	Rozumie czynniki ludzkie: błędy ludzkie, czynniki psychospołeczne, kultura bezpieczeństwa, wellbeing, Safety-II	P6S_WG

Umiejętności

Symbol KEU	Kierunkowe efekty uczenia się	Symbol CEU
ZZBPSP_U01	Potrafi przeprowadzać ocenę ryzyka operacyjnego (zawodowe, cyber, fraud, insider, szpiegostwo, fizyczne) i proponować adekwatne, proporcjonalne środki zaradcze	P6S_UW
ZZBPSP_U02	Potrafi analizować i weryfikować informacje o kontrahentach, osobach i podmiotach (KYC analityczne, OSINT, grafy powiązań, triangulacja źródeł, raport z rekomendacjami)	P6S_UW
ZZBPSP_U03	Potrafi rozpoznawać aktualne metody cyberprzestępczości (phishing AI, ransomware, BEC z deepfake, ataki na łańcuch dostaw) i oceniać podatności organizacji	P6S_UW
ZZBPSP_U04	Potrafi projektować i wdrażać procedury bezpieczeństwa: polityki, plany BCP/DRP, procedury reagowania na incydent, checklisty anty-fraud i kontrwywiadowcze, procedury KD i monitoringu wizyjnego	P6S_UO
ZZBPSP_U05	Potrafi organizować reakcję na incydent bezpieczeństwa (cyber, fraud, wyciek, włamanie fizyczne): izolacja, containment, raportowanie do organów, komunikacja kryzysowa	P6S_UO
ZZBPSP_U06	Posiada umiejętność spójnego, logicznego, merytorycznego dokonywania wypowiedzi w mowie i piśmie na tematy dotyczące wybranych zagadnień z zakresu analizy kryminalnej, z wykorzystaniem wiedzy teoretyczno-praktycznej oraz w powiązaniu i odniesieniu do innych dyscyplin nauki	P6S_UK
ZZBPSP_U07	Potrafi przeprowadzać proste audyty zgodności (NIS2, DORA, RODO, ISO) oraz audyty zabezpieczeń fizycznych obiektu	P6S_UO
ZZBPSP_U08	Potrafi prowadzić szkolenia, kampanie świadomościowe i symulacje (table-top exercises) dla pracowników i kadry kierowniczej	P6S_UU

Symbol KEU	Kierunkowe efekty uczenia się	Symbol CEU
ZZBPSP_U09	Potrafi integrować ochronę fizyczną z cyberbezpieczeństwem i procedurami HR (np. automatyczna blokada dostępu po zwolnieniu)	P6S_UW
ZZBPSP_U10	Potrafi funkcjonować i współdziałać w zespole i pod presją czasu	P6S_UO

Kompetencje społeczne

Symbol KEU	Kierunkowe efekty uczenia się	Symbol CEU
ZZBPSP_K01	Jest gotów podejmować odpowiedzialne decyzje w warunkach niepewności i presji czasowej, równoważąc bezpieczeństwo organizacji z prawami pracowników, proporcjonalnością środków i ochroną prywatności	P6S_KO
ZZBPSP_K02	Jest gotów promować i budować kulturę bezpieczeństwa („see something – say something”, whistleblowing bez atmosfery donosicielstwa, przeciwdziałanie mobbingowi i czynnikom psychospołecznym, wellbeing)	P6S_KR
ZZBPSP_K03	Jest gotów działać etycznie i proporcjonalnie (etyka monitoringu wizyjnego, kontroli dostępu biometrycznego, monitoringu behawioralnego, analizy OSINT)	P6S_KO
ZZBPSP_K04	Jest gotów skutecznie komunikować się w sytuacjach kryzysowych – wewnętrznie (zarząd, pracownicy) i zewnętrznie (organy nadzoru, ubezpieczyciele, media)	P6S_KR
ZZBPSP_K05	Jest gotów krytycznie oceniać własne kompetencje oraz skuteczność wdrożonych rozwiązań i samodzielnie planować ich doskonalenie	P6S_KK
ZZBPSP_K06	Jest gotów inicjować i wspierać działania poprawiające bezpieczeństwo w przedsiębiorstwie oraz w relacjach z kontrahentami i otoczeniem biznesowym	P6S_KR