UNIWERSYTET
Andrzeja Frycza Modrzewskiego
w Krakowie

KARTA PRZEDMIOTU

1. Informacje wstępne

Nazwa przedmiotu	**Audyt bezpieczeństwa Informacji**
Wydział	Wydział Zarządzania, Mediów i Technologii
Kierunek	Informatyka i ekonometria
Specjalność/Ścieżka specjalizacyjna	bezpieczeństwo informacji
Poziom PRK	6 PRK
Poziom kształcenia	studia pierwszego stopnia
Forma studiów	studia niestacjonarne
Grupa zajęć	—
Liczba punktów ECTS	5
Rodzaj przedmiotu	specjalizacyjny
Liczba godzin ogółem	45 godz.
Cykl dydaktyczny	2021/2022 zimowy
Semestr studiów	7
Rok studiów	4
Profil kształcenia	praktyczny
Rok realizacji	2024/2025
Język wykładowy	polski
Osoba odpowiedzialna za przedmiot	mgr Roman Jezierski (e-mail: rjezierski@uafm.edu.pl)

Semestr, liczba punktów ECTS, rodzaj zajęć, liczba godzin w planie studiów

Semestr	Wykład	Laboratorium	ECTS
7	15 godz.	30 godz.	5

2. Cele przedmiotu

C1	Przekazanie wiedzy związanej z organizacją i przebiegiem audytu bezpieczeństwa klauzulowanych informacji i stanowiących tajemnice prawnie chronione przetwarzanych w niejawnych systemach informatycznych.

3. Wymagania wstępne

Brak wymagań wstępnych.

4. Opis efektów uczenia się

W1	Wiedza: Zna i rozumie wymagania bezpieczeństwa tajemnic prawnie chronionych i informacji niejawnych przetwarzanych w systemach informatycznych.	EUK6_W1, EUK6_W2, EUK6_W3, EUK6_W4, EUK6_W5, EUK6_W6, EUK6_W7
W2	Wiedza: Zna podstawowe obowiązki personelu bezpieczeństwa w rozumieniu ustawy o ochronie informacji niejawnych i aktów wykonawczych w zakresie podstawowych wymagań bezpieczeństwa informatycznego.	EUK6_W1, EUK6_W2, EUK6_W3, EUK6_W4, EUK6_W5, EUK6_W6, EUK6_W7
U1	Umiejętności: Umie interpretować przepisy regulujące bezpieczeństwo informatyczne.	EUK6_U1, EUK6_U2, EUK6_U3, EUK6_U4, EUK6_U5, EUK6_U6, EUK6_U7, EUK6_U8
U2	Umiejętności: Potrafi określić zadania personelowi bezpieczeństwa dotyczące przygotowania się do procesu akredytacyjnego w zakresie wdrożonych procedur i rozwiązań zapewniających bezpieczeństwo danych.	EUK6_U1, EUK6_U2, EUK6_U3, EUK6_U4, EUK6_U5, EUK6_U6, EUK6_U7, EUK6_U8
K1	Kompetencje społeczne: Ma zdolność do pogłębiania wiedzy i na bieżąco analizuje zmiany aktów prawnych i przepisów wykonawczych w dziedzinie bezpieczeństwa informacji.	EUK6_KS1, EUK6_KS2, EUK6_KS3, EUK6_KS4
K2	Kompetencje społeczne: Wykorzystuje nabytą wiedzę i umiejętności do zapewnienia właściwego poziomu bezpieczeństwa danych.	EUK6_KS1, EUK6_KS2, EUK6_KS3, EUK6_KS4

5. Treści programowe

Wykład (15 godz.)

Kod	Tematyka zajęć (nr semestru: 7)
Wyk1	Bezpieczeństwo teleinformatyczne na mocy przepisów ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych. - 3 godz.
Wyk2	Etapy organizacji funkcjonowania niejawnych systemów informatycznych. - 2 godz.
Wyk3	Obowiązki personelu bezpieczeństwa w zakresie funkcjonowania jawnych i niejawnych systemów informatycznych - 2 godz.
Wyk4	Dokumentacja ogólnosystemowa systemów informatycznych - 2 godz.
Wyk5	Elementy polityki bezpieczeństwa - 2 godz.
Wyk6	Przedsięwzięcia organizacyjne kierownika jednostki organizacyjnej w zakresie przygotowania i przebiegu audytu niejawnego systemu informatycznego - 2 godz.
Wyk7	Materiał dowodowy poddany sprawdzeniu w ramach audytu - 2 godz.

Laboratorium (30 godz.)

Kod	Tematyka zajęć (nr semestru: 7)
Lab1	Polityka bezpieczeństwa informacji w jednostce organizacyjnej - 3 godz.
Lab2	Środki bezpieczeństwa fizycznego jednostki organizacyjnej w zakresie bezpieczeństwa teleinformatycznego - 3 godz.
Lab3	Środki bezpieczeństwa technicznego jednostki organizacyjnej w zakresie bezpieczeństwa teleinformatycznego - 3 godz.
Lab4	Norma PN-EN ISO/IEC 27001 System Zarządzania Bezpieczeństwem Informacji - 2 godz.
Lab5	Norma PN-EN ISO 9001 System zarządzania jakością - 2 godz.
Lab6	Elementy Zarządzania Bezpieczeństwem Informacji - 3 godz.
Lab7	Procedury Bezpiecznej Eksploatacji wybranego niejawnego systemu informatycznego - 2 godz.
Lab8	Audyt wewnętrzny i zewnętrzny w zakresie bezpieczeństwa informacji - 4 godz.
Lab9	Organizacja systemu ochrony danych i informacji niejawnych w czasie narad, odpraw, konferencji i rozmów - 2 godz.
Lab10	Opracowanie niezbędnych danych ujętych w „Planie ochrony informacji niejawnych.....…jednostki organizacyjnej” dotyczących bezpieczeństwa teleinformatycznego niejawnego systemu informatycznego - 4 godz.

Lab11	Sporządzenie arkuszy uzgodnień z Policją, Żandarmerią Wojskową oraz jednostką organizacyjną w zakresie ewakuacji niejawnych informatycznych nośników danych - 2 godz.

6. Metody dydaktyczne

Wykład	
M1	Analiza przypadków
M3	Burza mózgów
M6	Dyskusja
M16	Praca w grupach
M17	Prezentacja multimedialna
M20	Wykłady
M21	Wykorzystanie narzędzi nauczania zdalnego
M25	Pokaz
Laboratorium	
M3	Burza mózgów
M6	Dyskusja
M16	Praca w grupach
M17	Prezentacja multimedialna
M20	Uczenie się w oparciu o problem
M23	Zajęcia praktyczne

7. Nakład pracy studenta

Forma aktywności studenta	Obciążenie studenta
Wykład	**15 godz.**
W tym metodą e-learning:	**0 godz.**

Laboratorium	**30 godz.**
W tym metodą e-learning:	**0 godz.**

Praca własna studenta	
zapoznanie się z literaturą, Praca własna studenta- test, Praca własna studenta, przygotowanie projektu,	**80 godz.**

Całkowite obciążenia	
Sumaryczna liczba godzin dla przedmiotu wynikajaca z całego nakładu pracy studenta	**125 godz.**
Sumaryczna liczba punktów ECTS dla przedmiotu	**5 ECTS**

8. Kryteria oceny

Warunki zaliczenia przedmiotu:

Wykonanie i zaprezentowanie 3 projektów prezentacji w formie Power Point lub w formie Word w zakresie przedmiotu „Audyt Bezpieczeństwa Informacji ”.

Wykłady (Egzamin końcowy / Zaliczenie końcowe)	
Na ocenę 5:	Co najmniej 95% prawidłowo udzielonych odpowiedzi na pytania testowe.
Na ocenę 4,5:	Co najmniej 85% prawidłowo udzielonych odpowiedzi na pytania testowe.
Na ocenę 4:	Co najmniej 75% prawidłowo udzielonych odpowiedzi na pytania testowe.
Na ocenę 3,5:	Co najmniej 65% prawidłowo udzielonych odpowiedzi na pytania testowe.
Na ocenę 3:	Co najmniej 60% prawidłowo udzielonych odpowiedzi na pytania testowe.

Laboratorium	
Na ocenę 5:	Wyczerpujące opanowanie całego materiału programowego. Sprawnie wykorzystuje wiedzę. Umiejętnie dokonuje oceny problemów, procesów i zjawiska. Jest zainteresowany problematyką przedmiotu. Przejawia postawę racjonalną, krytyczną i kreatywną. Prace spełniają wymogi w zakresie istniejących przepisów i rozwiązań organizacyjnych ujętych w przepisach prawa.
Na ocenę 4,5:	Opanowanie całego materiału programowego. Przejawia zainteresowania w zakresie rozwiązywania problemów. Na obniżenie ww. oceny wpływają niżej wymienione nieprawidłowości: - projekt prezentacji zawiera drobne uchybienia dotyczące bezpieczeństwa systemów informatycznych i polityki bezpieczeństwa.
Na ocenę 4:	Zakres wiedzy pozwala na identyfikację i prawidłową ocenę zadań kierowników jednostek organizacyjnych i personelu bezpieczeństwa w zakresie wdrażania i eksploatacji systemów informatycznych i polityki bezpieczeństwa. Na obniżenie ww. oceny wpływają niżej wymienione nieprawidłowości: - pominięto rozwiązania organizacyjne opisujące zagrożenia dla bezpieczeństwa systemów i danych.
Na ocenę 3,5:	Poprawnie rozumie pojęcia, rozróżnia źródła prawa i przepisów wewnętrznych i prawidłowo objaśnia ich znaczenie. Przejawia przeciętną aktywność. Na obniżenie ww. oceny wpływają niżej wymienione nieprawidłowości: - przyjęte rozwiązania ujęte w pracy są zbyt lakoniczne, - mało merytoryczna treść projektów prezentacji.
Na ocenę 3:	Wykazuje braki w wiedzy, które jednak nie umożliwiają dalszej edukacji i mogą zostać usunięte. Rozwiązuje problemy typowe o niewielkim stopniu trudności. Pracuje niesystematycznie. Na obniżenie ww. oceny wpływają niżej wymienione nieprawidłowości: - nie zachowanie układu agendy prezentacji, - brak źródeł odniesień (kłopoty z prawem autorskim), - odczytanie prezentacji (tzw. ściana tekstu).

9. Literatura

Literatura podstawowa

1. R. Baltowski, Bezpieczeństwo systemów teleinformatycznych – zmiany, trendy i zasady, Warszawa 2018 NOVUM.
2. L. Brown, W. Stallings, Bezpieczeństwo systemów informatycznych. Zasady i praktyka. Tom 2 wyd. 4, 2023 r. Hellion.
3. J. Rembikowski, Audyt systemów informatycznych w ramach Polityki Bezpieczeństwa Informacji, Poznań, 2010 r. FORUM.

Literatura uzupełniająca

1. T. Polaczek, Audyt bezpieczeństwa informacji w praktyce, Helion, Gliwice 2006.
2. J. Krawiec, G. Ożarek: System Zarządzania Bezpieczeństwem Informacji w praktyce. Zabezpieczenia (Wydanie II zaktualizowane i rozszerzone). Wyd. PKN, Warszawa 2014.
3. . Lisiak-Felicka, M. Szmit, Cyberbezpieczeństwo administracji publicznej w Polsce, EAS, Kraków 2016.

Pomoce dodatkowe

1. Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. 2024 r. poz. 632 z późn. zm.).
2. Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 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 .
3. Rozporządzenie Prezesa Rady Ministrów z dnia 20 lipca 2011 r. w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego (Dz. U. z 2011 r. Nr 159, poz. 948).
4. Rozporządzenie Rady Ministrów z dnia 29 maja 2012 r. w sprawie środków bezpieczeństwa fizycznego stosowanych do zabezpieczenia informacji niejawnych (Dz. U. z 2012 r. poz. 683 z późn. zm.).
5. Rozporządzenie Ministra Obrony Narodowej z dnia 19 grudnia 2013 r. w sprawie szczegółowych zadań pełnomocników ochrony w zakresie ochrony informacji niejawnych w jednostkach organizacyjnych podległych Ministrowi Obrony Narodowej lub przez niego nadzorowanych (Dz. Urz. Min. Obr. Nar. z 2022 r. poz. 322 - j.t.).
6. Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U z 2024 r. poz. 733 – t.j.)
7. Norma PN-EN ISO/IEC 27001:2017 System Zarzadzania Bezpieczeństwem Informacji.
8. Norma PN-EN ISO/IEC 27002:2013 Zabezpieczenia.
9. Norma PN-EN ISO 9001 - System zarzadzania jakością.

10. Informacje dodatkowe dla studentów

mgr Roman Jezierski e-mail: rjezierski@uafm.edu.pl

11. Informacja o osobach prowadzących zajęcia

Osoby prowadzące zajęcia

mgr Roman Jezierski (e-mail: rjezierski@uafm.edu.pl)