2

Program studiów

Cyberbezpieczeństwo i ochrona zasobów informacyjnych

podyplomowe

1. Podstawowe informacje o studiach podyplomowych

Nazwa studiów	**Cyberbezpieczeństwo i ochrona zasobów informacyjnych**
Poziom studiów	**podyplomowe**
Liczba semestrów	studia niestacjonarne: **2**
Liczba punktów ECTS wymagana do ukończenia studiów	**30**
Łączna liczba godzin zajęć	**233**

2. Cel studiów podyplomowych

Cyberbezpieczenstwo jest kluczowym zagadnieniem we współczesnym cyfrowym świecie. Brak zapewnienia odpowiednich działań może poważnie zagrozić dalszemu rozwojowi i bezpieczeństwu organizacji. Zaistniała sytuacja wymusza odpowiednio przygotowanej kadry odpowiedzialnej za politykę bezpieczeństwa w instytucji, która na bieżąco będzie analizować aspekty bezpieczeństwa informatycznego i dostosowywać rozwiązania adekwatne do nowych wymagań. Przyszli administratorzy powinni być zaznajomieni z zagrożeniami systemów informatycznych w kontekście poufności, integralności i dostępności informacji oraz z możliwościami konfiguracyjnymi infrastruktury sprzętowo-programowej mającej na celu zapewnienie bezpieczeństwa instytucji. Zapewnienie współczesnym sieciom i systemom odpowiedniego poziomu bezpieczeństwa wymaga już nie tylko zarządzania aktualizacjami czy oprogramowaniem antywirusowym. Potrzebna jest weryfikacja w celu określenia, które elementy systemu są podatne na zagrożenia. Dodatkowo rozwój technologii mobilnych, stosowanie polityki BYOD, intensywny wzrost znaczenia systemów e-commerce powoduje nowe zagrożenia, które wymagają nowego podejścia do ochrony informacji. W konsekwencji przekłada się to na konieczność odpowiedniego przygotowania kadry odpowiedzialnej za politykę bezpieczeństwa w instytucji, która na bieżąco będzie analizować aspekty bezpieczeństwa informatycznego i dostosowywać rozwiązania adekwatne do nowych wymagań. Zaproponowane studia pozwolą słuchaczom zaznajomienie się z zagrożeniami systemów informatycznych w kontekście poufności, integralności i dostępności informacji oraz z możliwościami konfiguracyjnymi infrastruktury sprzętowo-programowej mającej na celu zapewnienie bezpieczeństwa instytucji.

3. Adresaci studiów podyplomowych

Adresatami studiów podyplomowych są absolwenci uczelni wyższych, a szczególnie praktycy stykający się w swojej pracy zawodowej z problemami związanymi z ochroną zasobów informacyjnych zainteresowani udziałem w studiach.

4. Sylwetka absolwenta, możliwości zatrudnienia

Absolwent jest w stanie sprawnie identyfikować zagrożenia bezpieczeństwa systemów informacyjnych, potrafi wskazać najlepsze rozwiązania w zakresie ochrony bezpieczeństwa informacji, a także potrafi projektować i wdrażać systemy bezpieczeństwa informacji. Zyska umiejętności pozwalające na analizę przyczyn i przebiegu procesów, a także zjawisk społecznych, które pozwolą na formułowanie własnych opinii. Potrafi również wykorzystać wiedzę teoretyczną do opisu i analizy przyczyn i przebiegu procesów związanych z bezpieczeństwem w cyberprzestrzeni.
Absolwent uzyska następującą wiedzę i umiejętności:
Wiedza:

- Podstawy prawne cyberbezpieczeństwa.
- Współczesne koncepcje bezpieczeństwa.
- Ochrona informacji niejawnych.
- Metody, techniki i narzędzia bezpieczeństwa informacji.
- Zagrożenia bezpieczeństwa informacji i ich źródła.
- Informacja, dezinformacja, manipulacja.
- Cyberbezpieczeństwo infrastruktury krytycznej.
- Systemy zarządzania bezpieczeństwem informacji.
- Administracja systemów operacyjnych.
- Systemy i sieci teleinformatyczne.
- Testy penetracyjne sieci, serwerów i aplikacji.
- Eksploatacja i bezpieczeństwo systemów bazodanowych.

Umiejętności:

- Zdolność identyfikacji zagrożeń bezpieczeństwa informacji.
- Umiejętność wskazywania najlepszych rozwiązań w zakresie ochrony bezpieczeństwa informacji.
- Zdolność do pozyskiwania, gromadzenia, przetwarzania informacji zgodnie z obowiązującymi normami i zasadami.
- Zdolność identyfikacji zagrożeń bezpieczeństwa systemów informacyjnych.
- Projektowanie i wdrażanie systemów ochrony informacji.
- Zdolność zarządzania ryzykiem.
- Zdolność zarządzania projektami.

5. Zasady rekrutacji

Rekrutacja na studia podyplomowe odbywa się w Systemie Internetowej Rekrutacji kandydatów „SIR" przez stronę internetową: www.prz.edu.pl. Rejestracja kandydata w SIR jest warunkiem przystąpienia do postępowania kwalifikacyjnego. Rekrutacja przebiega bez egzaminów wstępnych. O przyjęciu decyduje pozytywna weryfikacja dokumentów złożonych przez kandydata, a w przypadku większej liczby kandydatów niż liczba miejsc określona w limitach, o przyjęciu decyduje kolejność złożenia kompletu wymaganych dokumentów w wyznaczonym terminie.
Miejsce składania dokumentów: Biuro Centrum Studiów Podyplomowych Wydziału Zarządzania.
Kandydaci składają:
1) ankietę osobową (formularz PODANIA SIR) – wydrukowaną z Systemu Internetowej Rekrutacji i podpisaną przez kandydata,
2) kopię dyplomu ukończenia studiów wyższych – oryginał dyplomu należy przedstawić do wglądu kierownikowi lub osobie przez niego upoważnionej w celu poświadczenia zgodności kopii składanego dokumentu z jego oryginałem;
3) oświadczenie dotyczące pokrycia kosztów kształcenia, w przypadku gdy koszty kształcenia pokrywa pracodawca.
Niedostarczenie w ustalonym terminie kompletu dokumentów skutkuje niedopuszczeniem kandydata do dalszego postępowania rekrutacyjnego.

6. Efekty uczenia się

Symbol	Treść	Odniesienia do PRK
K_W01	Ma wiedzę na temat systemów zarządzania bezpieczeństwem informacji zgodnie z obowiązującymi normami.	**P6S_WG**
K_W02	Zna metody, techniki i narzędzia zapewniania bezpieczeństwa informacji.	**P7S_WG**
K_W03	Zna zagrożenia bezpieczeństwa informacji i ich źródła	**P7S_WG**

K_U01	Potrafi identyfikować zagrożenia bezpieczeństwa informacji	**P7S_UW**
K_U02	Umie wskazać najlepsze rozwiązania w zakresie ochrony bezpieczeństwa informacji.	**P7S_UW**
K_U03	Potrafi pozyskiwać, gromadzić i przetwarzać informacje zgodnie z obowiązującymi normami i zasadami.	**P7S_UW** **P7S_UU**
K_U04	Identyfikuje zagrożenia bezpieczeństwa systemów informacyjnych.	**P7S_UW**
K_U05	Potrafi projektować i wdrażać systemy ochrony informacji.	**P7S_UW**
K_K01	Ma świadomość odpowiedzialności za bezpieczeństwo informacji oraz swojej roli w jego zapewnieniu.	**P7S_KO**
K_K02	Ma świadomość stałego podnoszenia swoich kompetencji z zakresu ochrony informacji, również przy wykorzystaniu opinii ekspertów.	**P7S_KK**

Opis efektów uczenia się zawiera efekty uczenia się, o których mowa w ustawie z dnia 22 grudnia 2015 r. o Zintegrowanym Systemie Kwalifikacji i uwzględnienia uniwersalne charakterystyki pierwszego stopnia określone w tej ustawie oraz charakterystyki drugiego stopnia określone w przepisach wydanych na podstawie art. 7 ust. 3 tej ustawy.

7. Wykaz zajęć, parametry programu studiów, metody weryfikacji efektów uczenia się oraz treści programowe

7.1 Wykaz zajęć

Sem.	Jedn.	Nazwa zajęć	Wykład	Ćwiczenia/ Lektorat	Lab.	Projekt/ Seminarium	Suma godzin	Punkty ECTS	Godziny praktyczne	ECTS praktyczne	Godziny zdalne	ECTS zdalne	Egzamin	Oblig.
1	ES	Audyt informatyczny	10	0	0	0	10	1	0	0	10	1	N	
1	EU	Metody zapewniania bezpieczeństw systemów operacyjnych	8	0	12	0	20	2	12	1	8	1	N	
1	ZE	Ochrona informacji niejawnych	10	0	0	0	10	1	0	0	10	1	N	
1	ES	Ochrona sieci komputerowych	8	0	12	0	20	3	12	2	8	1	T	
1	ZE	Podstawy prawne cyberprzestrzeni w UE oraz Polsce	8	8	0	0	16	2	8	1	16	2	N	
1	ZE	Strategia ochrony cyberprzestrzeni Polski	8	8	0	0	16	2	8	1	8	1	N	
1	ZE	Współczesne koncepcje bezpieczeństwa oraz globalne trendy gospodarcze	8	8	0	0	16	2	8	1	0	0	T	
1	ZE	Zarządzanie projektami	8	8	0	0	16	2	8	1	0	0	N	
Sumy za semestr: 1			**68**	**32**	**24**	**0**	**124**	**15**	**56**	**7**	**60**	**7**	**2**	**0**
2	ES	Cyberbezpieczeństwo infrastruktury krytycznej - projekcja zagrożeń	0	0	0	5	5	1	5	1	5	1	T	
2	ES	Eksploatacja i bezpieczeństwo systemów bazodanowych	8	0	6	0	14	2	6	1	8	1	N	
2	ZE	Internet - informacja, dezinformacja, manipulacja	11	11	0	0	22	2	11	1	11	1	T	
2	ES	Nowoczesne metody monitoringu włamań w systemach teleinformatycznych	6	0	10	0	16	2	10	1	6	1	N	
2	ES	Testy penetracyjne aplikacji webowych, systemów i sieci	6	0	6	0	12	3	6	2	6	2	N	
2	ZE	Zarządzanie i audytowanie bezpieczeństwa informacji zgodnie z normą ISO 27001	12	12	0	0	24	3	12	2	24	3	N	
2	ES	Zarządzanie incydentami - SOC oraz CERT	6	0	10	0	16	2	10	1	6	1	N	
Sumy za semestr: 2			**49**	**23**	**32**	**5**	**109**	**15**	**60**	**9**	**66**	**10**	**2**	**0**
SUMY ZA WSZYSTKIE SEMESTRY:			**117**	**55**	**56**	**5**	**233**	**30**	**116**	**16**	**126**	**17**	**4**	**0**

Liczba punktów ECTS przypisanych do zajęć kształtujących umiejętności praktyczne: **16**
Liczba punktów ECTS przypisanych do zajęć prowadzonych z wykorzystaniem metod i technik kształcenia na odległość: **17**

7.2 Parametry programu studiów i metody weryfikacji efektów uczenia się

Parametry programu studiów

Łączna liczba punktów ECTS, którą student musi uzyskać w ramach zajęć prowadzonych z bezpośrednim udziałem nauczycieli akademickich lub innych osób prowadzących zajęcia.	11 ECTS
Łączna liczba punktów ECTS przyporządkowana zajęciom związanym z prowadzoną w uczelni działalnością naukową w dyscyplinie lub dyscyplinach, do których przyporządkowany jest kierunek studiów.	16 ECTS
Łączna liczba punktów ECTS, jaką student musi uzyskać w ramach zajęć z dziedziny nauk humanistycznych lub nauk społecznych w przypadku kierunków studiów przyporządkowanych do dyscyplin w ramach dziedzin innych niż odpowiednio nauki humanistyczne lub nauki społeczne.	--
Łączna liczba punktów ECTS przyporządkowana przedmiotom do wyboru.	0 ECTS
Liczba godzin zajęć z wychowania fizycznego.	--

Metody weryfikacji efektów uczenia się

Szczegółowe zasady oraz metody weryfikacji i oceny efektów uczenia się pozwalające na sprawdzenie i ocenę wszystkich efektów uczenia się są opisane w kartach zajęć. W ramach programu weryfikacja osiąganych efektów uczenia się jest realizowana w szczególności przy pomocy następujących metod: egzamin cz. pisemna, egzamin cz. praktyczna, egzamin cz. ustna, zaliczenie cz. pisemna, zaliczenie cz. praktyczna, zaliczenie cz. ustna, esej, kolokwium, sprawdzian pisemny, obserwacja wykonawstwa, prezentacja dokonań (portfolio), prezentacja projektu, raport pisemny, referat pisemny, referat ustny, sprawozdanie z projektu, test pisemny. Szczegółowe informacje na temat weryfikacji osiąganych przez studentów efektów uczenia się znajdują się w kartach zajęć opublikowanych na stronie internetowej wydziału. Parametry wybranych metod weryfikacji efektów uczenia się znajdują się w tabeli poniżej.

Liczba zajęć, w których wymagany jest egzamin	4
Liczba zajęć, w których wymagany jest egzamin w formie pisemnej	2
Liczba zajęć, w których wymagany jest egzamin w formie ustnej	0
Liczba godzin przeznaczona na egzamin w formie pisemnej	3
Liczba godzin przeznaczona na egzamin w formie ustnej	0
Szacowana liczba godzin, którą studenci powinni poświęcić na przygotowanie się do egzaminów i zaliczeń	108
Liczba zajęć, które kończą się zaliczeniem bez egzaminu	11
Liczba godzin przeznaczona na zaliczenie w formie pisemnej	10
Liczba godzin przeznaczona na zaliczenie w formie ustnej	6
Szacowana liczba godzin, którą studenci powinni poświęcić na przygotowanie się do zaliczeń w trakcie semestrów na zajęciach ćwiczeniowych (bez zaliczeń końcowych)	8
Liczba zajęć, w których weryfikacja osiąganych efektów uczenia się realizowana jest na podstawie obserwacji wykonawstwa (laboratoria)	6
Liczba laboratoriów, w których osiągane efekty uczenia się sprawdzane są na podstawie sprawdzianów w trakcie semestru	6
Szacowana liczba godzin, którą studenci powinni poświęcić na przygotowanie się do sprawdzianów realizowanych na zajęciach laboratoryjnych	31
Liczba zajęć projektowych, w których osiągane efekty uczenia się sprawdzane są na podstawie prezentacji projektu, raportu pisemnego, referatu pisemnego, referatu ustnego lub sprawozdania z projektu	1
Szacowana liczba godzin, którą studenci powinni poświęcić na wykonanie projektu/dokumentacji/raportu oraz przygotowanie do prezentacji	10
Liczba zajęć wykładowych, które wymagają odrębnego zaliczenia w formie pisemnej lub ustnej niezależnie od wymagań innych form zajęć tego modułu	8
Szacowana liczba godzin, którą studenci powinni poświęcić na przygotowanie się do sprawdzianów realizowanych na zajęciach wykładowych	54

7.3 Treści programowe

Audyt informatyczny	K_W01, K_U01, K_K02
• Cele audytu, aspekty prawne, standard ISO/IEC 27001. • Przegląd i charakterystyka narzędzi wykorzystywanych w audycie. • Dokumentacja poaudytowa, analiza i przygotowanie raportu i zaleceń.	
Cyberbezpieczeństwo infrastruktury krytycznej - projekcja zagrożeń	K_W03, K_U01, K_K01
• Znaczenie infrastruktury krytycznej • Rola systemów teleinformatycznych w zakresie infrastruktury krytycznej • Projekcja zagrożeń cybernetycznych dla infrastruktury krytycznej	
Eksploatacja i bezpieczeństwo systemów bazodanowych	K_W01, K_U05, K_K01
• Zajęcia organizacyjne. Ustalenie formy zaliczenia i zakresu materiału. Zapoznanie z regulaminem pracy w laboratorium. • Architektura systemów bazodanowych na przykładzie bazy danych Oracle: struktura serwera baz danych, połączenie z bazą danych, struktura pamięci, bufory bazy danych, obszar współdzielony, procesy pierwszo i drugoplanowe, logiczna i fizyczna struktura danych, przestrzenie tabel, segmenty, extenty i bloki. • Zarządzanie schematami: przydzielanie schematów, specyfikacja typów danych w tabelah, tworzenie, usuwanie i modyfikowanie tabel, integralność danych, więzy integralności, indeksy oraz ich typy (B-drzewo, bitmapa), widoki, sekwencje, synonimy, tabele tymczasowe. • Zarządzanie bezpieczeństwem użytkowników: konto użytkownika bazy danych, predefiniowane konta: sys i system, tworzenie, usuwanie, blokowanie i zarządzanie kontem użytkownika, resetowanie hasła, autentyfikacja użytkowników, zasada najmniejszych uprawnień i jej stosowanie, ochrona uprzywilejowanych kont, przywileje: systemowe, obiektowe, role, nadawanie, odbieranie i zarządzanie przywilejami na poziomie użytkownika oraz roli, tworzenie oraz zarządzanie rolami, implementacja cech bezpieczeństwa haseł, przydzielanie quotas użytkownikom. • Koncepcja backup'u i odtwarzania: kategorie uszkodzeń, proces punktu kontrolnego (CKPT), LogWriter i pliki Redo Log, asystent MTTR, zwielokrotnianie plików kontrolnych, proces archiwizacji i plik Archive Log, tryb archivelog, przenoszenie danych, metody importu i exportu danych.	

Internet - informacja, dezinformacja, manipulacja	K_W02, K_U02, K_K02
• Polityka informacji, dezinformacji oraz manipulacji • Walka i wojna informacyjna • Analiza informacji na przykładzie opisu współczesnych konfliktów. Działania w sieci. Działania hybrydowe. Oddziaływanie na ludzi przez media społecznościowe.	
Metody zapewniania bezpieczeństw systemów operacyjnych	K_W01, K_U03, K_U05, K_K02
• Zajęcia organizacyjne. Ustalenie formy zaliczenia i zakresu materiału. Zapoznanie z regulaminem pracy w laboratorium. Zarządzanie wbudowanymi kontami i grupami użytkowników i administratorów przy użyciu polityk systemowych i dedykowanych narzędzi. Tworzenie i wykorzystanie bezpiecznych kont usługowych działających w systemie operacyjnym. • Bezpieczne aktualizacje systemów operacyjnych w sposób kontrolowany w skali organizacji. Sprawdzanie systemów i aplikacji przy użyciu narzędzia analizy najlepszych praktyk (Best Practices Analyzer). Ochrona systemów operacyjnych poprzez ograniczanie uprawnień użytkowników oraz zarządzanie ustawieniami systemu i grupami użytkowników w automatyczny sposób przy użyciu polityk. • Wdrażanie szyfrowania dysków i plików w bezpieczny sposób w skali dużegej organizacji. Podstawy zarządzania certyfikatami w systemie operacyjnym. Ograniczanie podatności na ataki złośliwego oprogramowania poprzez kontrolowanie aplikacji przy użyciu i polityk systemu operacyjnego. • Narzędzia do detekcji podejrzanej aktywności w systemie operacyjnym. Zaawansowana inspekcja zdarzeń w systemie operacyjnym. Centralne zbieranie logów z systemów operacyjnych i interpretacja wpisów. Konfiguracja Windows Rejestru zdarzeń systemu.	
Nowoczesne metody monitoringu włamań w systemach teleinformatycznych	K_W01, K_W02, K_W03, K_U01, K_U02, K_U04, K_U05, K_K01, K_K02
• Zajęcia organizacyjne. Ustalenie formy zaliczenia i zakresu materiału. Zapoznanie z regulaminem pracy w laboratorium. Omówienie zagadnień z deszyfracja i monitorowaniem ruch przechodzącego przez zapory ogniowe. • Analiza zagrożeń wirusowych. Integracja WildFire z architekturą bezpieczeństwa, badanie zawartość plików i budowa bazy danych sygnatur wirusów. • Identyfikacja użytkownika końcowego. Zapoznanie się z konfiguracją zapory nowej generacji i uwierzytelnianiem identyfikatora użytkownika, a także z monitorowaniem i rejestrowaniem oraz mapowania identyfikatora użytkownika do urządzenia. • Bezpieczeństwo zdalnego dostępu. Konfiguracja certyfikatów uwierzytelniania zapory, profile bezpieczeństwa i agenci klienta. Monitorowanie i raportowanie bezpieczeństwa. Konfiguracja pulpitu nawigacyjnego oraz filtrów zapory. • Zapewnienie wysokiej dostępność urządzenia zabezpieczającego. Konfiguracja przypisania portów zapory w celu kontroli wysokiej dostępności, zarządzania i połączeń łącza danych.	
Ochrona informacji niejawnych	K_W01, K_U01, K_K01
• Zasady i standardy ochrony informacji niejawnych w Polsce oraz Unii Europejskiej. Definiowanie podstawowych pojęć dotyczących OIN. Klasyfikowanie informacji niejawnych. Zasady przetwarzania IN, Problematyka organizacji ochrony informacji niejawnych. Bezpieczeństwo osobowe. Bezpieczeństwo przemysłowe. Bezpieczeństwo w systemach i sieciach teleinformatycznych. Postępowanie odwoławcze. Kancelarie tajne - tryb ich tworzenia, organizacja pracy kancelarii tajnej.	
Ochrona sieci komputerowych	K_W01, K_W02, K_U03, K_K01
• Wprowadzenie do architektury funkcjonowania współczesnych sieci komputerowych • Mechanizmy adresacji wykorzystywane w sieciach komputerowych oraz modele ISO/OSI i TCP/IP. • Bezpieczeństwo sieci w warstwie 2 modelu ISO/OSI • Ruting i jego znaczenie dla bezpieczeństwa sieci komputerowych. • Metody i środki zabezpieczenia dostępu do sieci oraz do elementów infrastruktury sieciowej. Narzędzia diagnostyki. • Systemy klasy IPS i IDS • Rozwiązania VPN w sieciach komputerowych • Podsumowanie oraz case study	
Podstawy prawne cyberprzestrzeni w UE oraz Polsce	K_W01, K_W03, K_U01, K_U04, K_K01, K_K02
• Rola i znaczenie prawa. Źródła prawa. Specyfika prawa publicznego i prywatnego. Charakterystyka głównych gałęzi prawa. Odpowiedzialność prawna. Sposoby rozstrzygania sporów prawnych. • Cyberprzestępczość - zagadnienia ogólne. Pojęcie danych informatycznych. Pojęcie systemu informatycznego. Bezpieczeństwo danych informatycznych. Ochrona przed cyberprzestępczością na gruncie prawa unijnego. • Hacking komputerowy (art. 267 par. 1 k.k.) i nielegalny podsłuch komputerowy (art. 267 par. 2 k.k.) - podmiot przestępstwa, przedmiot przestępstwa, strona podmiotowa przestępstwa, strona przedmiotowa przestępstwa, karalność, ściganie. • Naruszenie integralności zapisu zapisu informacji (art. 268 par. 2 k.k.) i wyrządzenie szkody w danych informatycznych (art. 268a k.k.) - podmiot przestępstwa, przedmiot przestępstwa, strona podmiotowa przestępstwa, strona przedmiotowa przestępstwa, karalność, ściganie. • Sabotaż informatyczny (art. 269 k.k.) - podmiot przestępstwa, przedmiot przestępstwa, strona podmiotowa przestępstwa, strona przedmiotowa przestępstwa, karalność, ściganie. • Zakłócanie pracy w sieci (art. 269a k.k.) i bezprawne wykorzystanie programów i danych (art. 269b k.k.) - podmiot przestępstwa, przedmiot przestępstwa, strona podmiotowa przestępstwa, strona przedmiotowa przestępstwa, karalność, ściganie.	
Strategia ochrony cyberprzestrzeni Polski	K_W01, K_W03, K_U01, K_U02, K_K01, K_K02
• 1. Pojęcia : cyberterroryzm ,wojna hybrydowa, cyberprzestępczość, cyberprzestrzeń, polityka antycyberterrorystyczna, strategia cyberbezpieczeństwa 2. Doktryna cyberbezpieczeństwa RP i Unii Europejskiej • 3. Uwarunkowanie zjawisk cyberterrorystycznych 4.Źródła cyberterroryzmu, Cechy i mechanizmy cyberterroryzmu we współczesnym świecie • 5. Współczesna Strategia zwalczania terroryzmu i ochrony cyberprzestrzeni RP • 6.Realizacja polityki antycyberterrorystycznej na przykładzie RP 7. Procedury postępowania służb antyterrorystycznych w przypadku ataku cyberterrorystycznego na przykładzie innych wybranych państw UE • 8. Podstawy prawne polityki antycyberterrorystycznej w prawie międzynarodowym, unijnym i krajowym	
Testy penetracyjne aplikacji webowych, systemów i sieci	K_W01, K_W02, K_W03, K_U02, K_K02, K_K02
• Zajęcia organizacyjne. Ustalenie formy zaliczenia i zakresu materiału. Zapoznanie z regulaminem pracy w laboratorium. Wprowadzenie do testów penetracyjnych. Regulacje prawne dot. wykonywania testów penetracyjnych. • Metodyki testowania bezpieczeństwa systemów teleinformatycznych. Omówienie najczęściej występujących podatności aplikacji webowych, mobilnych i IoT. • Przegląd narzędzi do wykrywania luk bezpieczeństwa aplikacji. Fuzzing. Wykorzystywanie podatności w celu złamania zabezpieczeń aplikacji. • Omówienie najczęściej występujących ataków sieciowych. Omówienie fazy rekonesansu. Pasywne i aktywne zbieranie informacji. Analiza ruchu sieciowego. Przegląd narzędzi wykorzystywanych do testów penetracyjnych sieci. • Omówienie fazy ataku. Zapoznanie z narzędziami środowiska Kali Linux. Omówienie oprogramowania Metasploit. Przeprowadzanie ataków sieciowych, wykorzystanie podatności i przejęcie systemu. • Szacowanie ryzyka związanego z podatnością. Przygotowywanie raportów stanu bezpieczeństwa systemu. Atak socjotechniczny jako uzupełnienie testów penetracyjnych.	
Współczesne koncepcje bezpieczeństwa oraz globalne trendy gospodarcze	K_W01, K_W02, K_U01, K_K01
• Koncepcje bezpieczeństwa - wymiar teoretyczny • Charakterystyka współczesnych koncepcji bezpieczeństwa • Współczesne systemy bezpieczeństwa - studia przypadków • Systemy bezpieczeństwa wobec ataków cybernetycznych • Analiza informacji w obszarze bezpieczeństwa	
Zarządzanie i audytowanie bezpieczeństwa informacji zgodnie z normą ISO 27001	K_W01, K_U05, K_K01
• Zarządzanie bezpieczeństwem informacji. Atrybuty bezpieczeństwa informacji, korzyści, raporty. • Zagrożenia i przykłady incydentów BI. • Przedstawienie wymagań normy PN-EN ISO 27001:2023. • Audyt, niezgodności i potencjały doskonalenia. Audyty wewnętrzne. Program audytu. Role i odpowiedzialności podczas audytu. • Zamiany w bezpieczeństwie informacji, case study. • Proces audytu. Scenki audytowe.	
Zarządzanie incydentami - SOC oraz CERT	K_W01, K_W02, K_U03, K_K01

• Zajęcia organizacyjne. Ustalenie formy zaliczenia i zakresu materiału. Zapoznanie z regulaminem pracy w laboratorium. Przedstawienie podstawowej wiedzę z działu obsługi, sieci i konserwacji systemów, a także najlepsze praktyki w zakresie cyberbezpieczeństwa. • Diagnoza problemów z łącznością sieciową, w tym podsieciami, za pomocą powszechnie dostępnych narzędzi. Analiza przepływy ruchu sieciowego, przepustowość i wydajność za pomocą identyfikacji na poziomie pakietów. • Zagrożenia związane z cyberbezpieczeństwem. Rozpoznawanie słabych punktów i związane z nimi cyberzagrożenia. • Chmura, wirtualizacja i bezpieczeństwo pamięci masowej. Opracowanie i wdrażanie sieciowych procedur tworzenia kopii zapasowych i przywracania, zgodnych z planami odtwarzania po awarii. • Omówienie narzędzi do analizy i optymalizacji przepustowości sieci i zarządzania incydentami.	
Zarządzanie projektami	K_W02, K_U03, K_U05, K_K02
• Wprowadzenie do projektu, podejście systemowe do zarządzania projektami, przygotowanie, planowanie i controlling projektu. • Wykonanie projektu zespołowego	