

Załącznik nr 1
do uchwały nr 14/2020 Senatu
Politechniki Rzeszowskiej
z dnia 28 maja 2020 r.

Program studiów

Cyberbezpieczeństwo i ochrona zasobów informacyjnych

podyplomowe

Cykl kształcenia: 2020/2021

1. Podstawowe informacje o studiach podyplomowych

Nazwa studiów	Cyberbezpieczeństwo i ochrona zasobów informacyjnych
Poziom studiów	podyplomowe
Liczba semestrów	2
Liczba punktów ECTS wymagana do ukończenia studiów	30
Łączna liczba godzin zajęć	214

2. Cel studiów podyplomowych

Cyberbezpieczeństwo 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 zaznajomić 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. 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, w tym efekty w zakresie znajomości języka obcego, natomiast w przypadku kierunku studiów kończącego się uzyskaniem tytułu zawodowego inżyniera – pełen zakres efektów umożliwiających uzyskanie kompetencji inżynierskich.

6. Plany studiów, ich parametry, metody weryfikacji oraz treści kształcenia

6.1. Plan studiów

Semestr	Jedn.	Nazwa zajęć	Wykład	Ćwiczenia/ Lektorat	Laboratorium	Projekt/ Seminarium	Suma godzin	Punkty ECTS	Egzamin	Oblig.
1	ZE	Metody zapewniania bezpieczeństwa systemów operacyjnych	8	0	8	6	22	3	N	
1	ZE	Ochrona informacji niejawnych	8	0	0	0	8	1	N	
1	ZE	Ochrona sieci komputerowych	16	0	14	0	30	4	T	
1	ZE	Podstawy prawa	8	4	0	0	12	2	N	
1	ZE	Podstawy prawne cyberprzestrzeni w UE oraz Polsce	4	4	0	0	8	1	N	
1	ZE	Współczesne koncepcje bezpieczeństwa	6	6	0	0	12	2	T	
1	ZE	Zarządzanie projektami	4	4	0	8	16	2	N	
Sumy za semestr: 1			54	18	22	14	108	15	2	0
2	ZE	Ataki cybernetyczne - studia przypadków	4	12	0	0	16	2	N	
2	ZE	Bezpieczeństwo informatycznych systemów infrastruktury krytycznej	8	0	0	6	14	2	N	
2	ZE	Cyberbezpieczeństwo infrastruktury krytycznej - projekcja zagrożeń	8	0	0	8	16	2	T	
2	ZE	Eksploatacja i bezpieczeństwo systemów bazodanowych	8	0	6	0	14	2	N	
2	ZE	Internet - informacja, dezinformacja, manipulacja	8	8	0	0	16	2	T	
2	ZE	Testy penetracyjne aplikacji webowych, systemów i sieci	8	0	10	0	18	3	N	
2	ZE	Zarządzanie bezpieczeństwem informacji w przedsiębiorstwie	8	0	0	4	12	2	N	
Sumy za semestr: 2			52	20	16	18	106	15	2	0
SUMY ZA WSZYSTKIE SEMESTRY:			106	38	38	32	214	30	4	0

6.2. Sposoby 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 studiów weryfikacja osiągniętych 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.

Parametry wybranych metod weryfikacji efektów uczenia się

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 godz.
Liczba godzin przeznaczona na egzamin w formie ustnej	0 godz.
Szacowana liczba godzin, którą studenci powinni poświęcić na przygotowanie się do egzaminów i zaliczeń	108 godz.
Liczba zajęć, które kończą się zaliczeniem bez egzaminu	10
Liczba godzin przeznaczona na zaliczenie w formie pisemnej	8 godz.
Liczba godzin przeznaczona na zaliczenie w formie ustnej	1 godz.
Szacowana liczba godzin, którą studenci powinni poświęcić na przygotowanie się do zaliczeń w trakcie semestrów na zajęciach ćwiczeniowych (bez zaliczeń końcowych)	6 godz.
Liczba zajęć, w których weryfikacja osiągniętych efektów uczenia się realizowana jest na podstawie obserwacji wykonawstwa (laboratoria)	4
Liczba laboratoriów, w których osiągnięte efekty uczenia się sprawdzane są na podstawie sprawdzianów w trakcie semestru	3
Szacowana liczba godzin, którą studenci powinni poświęcić na przygotowanie się do sprawdzianów realizowanych na zajęciach laboratoryjnych	11 godz.
Liczba zajęć projektowych, w których osiągnięte efekty uczenia się sprawdzane są na podstawie prezentacji projektu, raportu pisemnego, referatu pisemnego, referatu ustnego lub sprawozdania z projektu	5
Szacowana liczba godzin, którą studenci powinni poświęcić na wykonanie projektu/dokumentacji/raportu oraz przygotowanie do prezentacji	84 godz.
Liczba zajęć wykładowych, które wymagają odrębnego zaliczenia w formie pisemnej lub ustnej niezależnie od wymagań innych form zajęć tego modułu.	9
Szacowana liczba godzin, którą studenci powinni poświęcić na przygotowanie się do sprawdzianów realizowanych na zajęciach wykładowych.	50 godz.

Szczegółowe informacje na temat weryfikacji osiągniętych przez studentów efektów uczenia się znajdują się w kartach zajęć pod adresem URL: <http://krk.prz.edu.pl/plany.pl?lng=PL&W=Z&K=ZCB&TK=html&S=1336&C=2019>

6.3. Treści programowe

Ataki cybernetyczne - studia przypadków	K_W01, K_W02, K_U04, K_K01
• Istota cyberataku • Atak cybernetyczny na infrastrukturę Ukrainy • Atak cybernetyczny na infrastrukturę Iranu	
Bezpieczeństwo informatycznych systemów infrastruktury krytycznej	K_W01, K_W02, K_W03, K_U01, K_U02, K_U04, K_U05, K_K01, K_K02
• Systemy infrastruktury krytycznej – wprowadzenie, uwarunkowania prawne, struktura • Fizyczna infrastruktura informatyczna o znaczeniu krytycznym • Chłodzenie jako element infrastruktury krytycznej • Zasilanie jako element infrastruktury krytycznej • Przykłady infrastruktury krytycznej - serwerownia, data center • Alternatywne technologie generowania mocy • Okablowanie strukturalne jako element infrastruktury krytycznej	
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	
Eksploracja 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 tabelach, 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 hasel, przydzielanie quotas użytkownikom. • Koncepcja backup'u i odtwarzania: kategorie uszkodzeń, proces punktu kontrolnego (CKPT), LogWriter i pliki Redo Log, asystent MTRR, 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 bezpieczeństwa systemów operacyjnych	K_W01, K_U03, K_U05, K_K02
• Zajęcia organizacyjne. Ustalenie formy zaliczenia i zakresu materiału. Zapoznanie z regulaminem pracy w laboratorium. 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 Event Collector. • Bezpieczne aktualizacje systemów operacyjnych w sposób kontrolowany w skali przedsiębiorstwa. Sprawdzanie systemów i aplikacji przy użyciu narzędzia Best Practices Analyzer. Ochrona systemów operacyjnych poprzez ograniczanie uprawnień użytkowników i zarządzanie grupami w automatyczny sposób przy użyciu Group Policy. • Zarządzanie wbudowanymi kontami administracyjnymi przy użyciu narzędzia Local Administrator Password Solutions. Tworzenie bezpiecznych kont dla usług działających w systemie operacyjnym. Wdrażanie szyfrowania plików w bezpieczny sposób w skali dużego przedsiębiorstwa. Zarządzanie kluczami. • Ograniczanie podatności na ataki złośliwego oprogramowania poprzez kontrolowanie aplikacji przy użyciu Software Restriction Policies i AppLocker.	
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 • Routing 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 prawa	K_W01, K_U01, K_K02
• Znaczenie, funkcje i podział prawa. • Istota prawa administracyjnego. • Istota prawa karnego.	
Podstawy prawne cyberprzestrzeni w UE oraz Polsce	K_W01, K_W03, K_U01, K_U04, K_K01, K_K02
• 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, 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.	
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	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	
Zarządzanie bezpieczeństwem informacji w przedsiębiorstwie	K_W01, K_W02, K_U03, K_K01
• Zarządzanie i organizacja bezpieczeństwa teleinformatycznego w przedsiębiorstwie (podstawowe pojęcia, role, podział odpowiedzialności, struktura organizacyjna). • Dokumentacja dotycząca bezpieczeństwa teleinformatycznego w przedsiębiorstwie (polityki, instrukcje, normy). • Domeny bezpieczeństwa teleinformatycznego w przedsiębiorstwie wraz z podstawowymi zabezpieczeniami (zarządzanie ryzykiem, bezpieczeństwo zasobów ludzkich, bezpieczeństwo infrastruktury teleinformatycznej, testy i audyty) • Zarządzanie incydentami związanymi z bezpieczeństwem informacji w przedsiębiorstwie • Zarządzanie ciągłością działania w kontekście bezpieczeństwa informacji	
Zarządzanie projektami	K_W02, K_U03, K_U05, K_K02
• Wprowadzenie do projektu, podejście systemowe do zarządzania projektami, przygotowanie, planowanie i controlling projektu. • Wykonanie	