ПЛОВДИВСКИ УНИВЕРСИТЕТ 1961 ПАИСИЙ ХИЛЕНДАРСКИ

ФАКУЛТЕТ ПО ИКОНОМИЧЕСКИ И СОЦИАЛНИ НАУКИ

УЧЕБЕН ПЛАН

на специалност

КИБЕРСИГУРНОСТ

редовно обучение

образователно-квалификационна степен „магистър“

Пловдивски университет „Паисий Хилендарски“
4000 Пловдив, ул. „Цар Асен“ 24

Факултет

Факултет икономически и социални науки

Професионално направление

Национална сигурност

Специалност

Киберсигурност

Форма на обучение

редовна

Утвърден с протокол на АС

No 13/2024-07-22

Утвърден с протокол на ФС

No 193/2024-07-12

Анотация

Магистърската програма осигурява на студентите знания и умения за справяне с най-новите заплахи и предизвикателства пред сигурността, каквито са заплахите в киберпространството. Програмата отговаря на европейските стандарти за обучение като осигурява: изучаване на теми в области като мениджмънт на киберсигурността, проектиране, изграждане и защита на информационни системи в частния и публичния сектор, приложение на информационните и комуникационни технологии в системите за сигурност.; стимулира аудиторната и самостоятелната работа на студентите посредством участието им в национални и международни проекти, стажове, семинари и конференции, с помощта на които се изграждат и затвърждават способности за творческа изява и работа в екип.
Обучението по магистърска програма "Киберсигурност" развива мисията на Университета, насочена към изграждане на специалисти със задълбочена подготовка, знания и умения. В магистърска програма "Киберсигурност" се подготвят специалисти в основни области от мениджмънта на киберсигурността: управление на риска, изграждане на способности за киберсигурност, управление на човешкият фактор в киберсигурността, противодействието срещу киберпрестъпления, интернет сигурност, мрежова и комуникационна сигурност и сигурност на системите на критичната информационна инфраструктура. Програмата е насочена към бизнес организацията (фирма, корпорация) и държавните органи и институции, към защита на отделния индивид, на националната и международна сигурност, както развитието на международно сътрудничество по проблемите на киберсигурността.

Професионална квалификация

Магистър по киберсигурност

Равнище на квалификация

Магистър

Специфични изисквания за достъп (прием)

- платено обучение;
- класиране по успех (минимален успех за кандидатстване Добър 3.50 от дипломата за ОКС „бакалавър“)

Ред за признаване на предходно обучение

- Диплома за завършено ОКС „Бакалавър”.
- Решение на комисията по признаване на кредити, получени в друг университет.

Квалификационни изисквания и правила за квалификация

За придобиване на квалификацията са необходими 109 кредита, от които:

- 94 кредита от задължителни, избираеми и факултативни дисциплини;
- 15 кредита за държавен изпит или защита на дипломна работа.

Профил на програмата (специалността)

Срокът на обучение е в рамките на три семестъра, (една и половина учебни години).

Основни резултати от обучението

Завършилите програмата притежават знания за:

- мениджмънта на киберсигурността, както и за методите, средствата за осигуряване на сигурност в киберпространството;
- информационните и комуникационните системи в сектора за сигурност и бизнес сектора и защитата на критичната информационна инфраструктура;
- изграждането и управлението на информационни системи и на ИТ проекти в публичния и частния сектор.

Те придобиват умения за:

- разработване и внедряване на защитени информационни системи;
- вземане на решение и разработване на системи за сигурност и защита на информационните ресурси;
-оценяване на риска и изграждане на способности в киберсигурността ;

Професионален профил на завършилите с примери

Завършилите магистърската програма "Киберсигурност" намират реализация в държавната администрация и в частния сектор като експерти и мениджъри по управление на киберсигурността, сигурност на информацията, компютърни и комуникационни технологии и системи, експерти по проектиране и разработване на информационни системи и такива за управление на информационната сигурност, както и в областта на защита на класифицираната информация.

Възможности за продължаване на обучението

В ОКС "доктор".

Диаграма на структурата на курсовете с кредити

Легенда

Аудиторни часове в семестъра/триместъра: **АО** - общ брой, от тях **Л** - за лекции; **С** - за семинарни (упражнения); **Лб** - за практикуми (лабораторни упражнения) и други часове **(Кл** - за колоквиуми,**Х** - за хоспетиране и пр.).

К - ECTS кредити: **ФИ -** форма на изпитване (със стойности И - изпит, Т - текуща оценка. З - заверка, П - продължава следващ семестър/триместър) **Код по ECTS -** виж поле 2. в ECTS макета

Извънаудиторни часове в семестъра/триместъра: **ИО** - общ брой, **Сп** - за самостоятелна работа/подготовка, и др..

No	Код по ECTS	Учебен курс / дисциплина	Аудиторни						Извънаудит.			К	Фи
			АО	Л	С	Лб	Кл	Х	ИО	Сп	...		
1	2	3	4	5	6	7	8	9	10	11	12	13	14
1-ви семестър													
1.		Въведение в киберсигурността (1)	30	30	0	0	0	0	120	120	0	6	И
2.		Въведение в мрежовата администрация (1)	30	15	15	0	0	0	120	120	0	6	И
3.		Управление на системите за киберсигурност (1)	30	30	0	0	0	0	120	120	0	6	И
4.		Стандарти за информационна сигурност (1)	30	30	0	0	0	0	120	120	0	6	И
5.		Избираема дисциплина (1)	30	15	15	0	0	0	120	120	0	6	И
Общо за 1-ви семестър			**150**	**120**	**30**	**0**	**0**	**0**	**600**	**600**	**0**	**30**	
2-ри семестър													
1.		Мрежова защита (1)	30	15	15	0	0	0	120	120	0	6	И
2.		Разследване на киберпрестъпления (1)	30	30	0	0	0	0	120	120	0	6	И
3.		Оперативен център за киберсигурност (SOC) (1)	30	15	15	0	0	0	120	120	0	6	И
4.		Етично хакерство (1)	30	15	15	0	0	0	120	120	0	6	И
5.		Факултативна дисциплина (1)	30	15	15	0	0	0	120	120	0	6	И
Общо за 2-ри семестър			**150**	**90**	**60**	**0**	**0**	**0**	**600**	**600**	**0**	**30**	
Общо за I-ва година			**300**	**210**	**90**	**0**	**0**	**0**	**1200**	**1200**	**0**	**60**	
3-ти семестър													
1.		Управление на риска и застраховане на киберативи (1)	30	30	0	0	0	0	120	120	0	6	И
2.		Екосистеми за сигурност (CERT) (1)	30	30	0	0	0	0	120	120	0	6	И
3.		Заплахи за киберсигурността (1)	30	15	15	0	0	0	120	120	0	6	И
4.		Компютърна криминалистика (1)	30	15	15	0	0	0	120	120	0	6	И
5.		Социално инженерство (1)	30	15	15	0	0	0	120	120	0	6	И
6.		Избираема дисциплина (1)	15	15	0	0	0	0	85	85	0	4	И
7.		Държавен изпит/Защита на дипломна работа (1)	0	0	0	0	0	0	375	375	0	15	И
Общо за 3-ти семестър			**165**	**120**	**45**	**0**	**0**	**0**	**1060**	**1060**	**0**	**49**	
Общо за целия курс на обучение			**465**	**330**	**135**	**0**	**0**	**0**	**2260**	**2260**	**0**	**109**	

Избираеми дисциплини

Избираема дисциплина (за семестър 1)
- Регулаторни изисквания за защита на личните данни
- Правна рамка на киберсигурността
Избираема дисциплина (за семестър 3)
- Методология за тестване на WEB приложения
- Практически аспекти на киберсигурността

Факултативни дисциплини

Факултативна дисциплина (за семестър 2)
- Дронове и сигурност
- Използване на трафични данни за разкриване на престъпления

Правила за изпитите, оценяване и поставяне на оценки

По време на обучението по всички научни дисциплини студентите се оценяват с текущи оценки на базата на: тестове, решаване на казуси и задължителни курсови работи, проекти и/или презентации. В края на обучението по даден курс студентите полагат писмен изпит. Указания за организацията и реда за провеждане на изпитите за всеки отделен курс са приложени в конкретната учебната програма. Семестриалната оценка се формира за всички курсове от текущата оценка и оценката от семестриалния изпит.
Държавен изпит /защита на дипломна работа/ по специалността

Форми за обучение

редовна