Специалност: **Киберсигурност и превенция на киберпрестъпления**

Код по ЕСНТК: **MCSPC**

Образователно-квалификационна степен: магистър-инженер по Киберсигурност и превенция на киберпрестъпления

Форма на обучение: задочна

Срок на обучение: 2 години (4 семестъра) за завършили образователно-квалификационна степен „бакалавър“ или „магистър“ по специалности от професионални направления 3.6. Право, 9. Сигурност и отбрана.

Завършване: с дипломен проект

Прием: на общо основание, съгласно действащия Правилник на ТУ – София.

Достъп до по-нататъшно обучение: на общо основание, съгласно действащия Правилник на ТУ – София.

Актуалност:

Специалността Киберсигурност и превенция на киберпрестъпления е изключително актуална в областта на компютрите и комуникациите и решаващата роля на киберсигурността в днешния цифров свят. Киберзаплахите в различни сектори, включително правителството, здравеопазването, финансите и технологиите нарастват по честота и сложност. Пробивите в киберсигурността и тяхното въздействие върху бизнеса и обществото са ежедневно и неотложно предизвикателство. Всичко това обуславя увеличеното търсене на специалисти по киберсигурност, тъй като организациите се стремят да защитят своите данни, инфраструктура и операции от кибератаки.

Обща характеристика на обучението:

Програмата дава знания, умения, навици, нагласи, ценности и компетенции, релевантни на съвременните бързо развиващи се компютърни технологии. Създават се възможност и условия за придобиване на знания и умения, покриващи интердисциплинарния характер в същността на киберсигурността. Дипломираните магистри следва да получат широк мироглед, способност за самостоятелна интерпретация и интердисциплинарен анализ на придобитите знания, да разбират, критично да възприемат и да излагат принципи и теории. Те следва да имат уменията да използват научни методи и средства за решаване на сложни задачи от професионалната и научна област на специалността, да прилагат придобитите знания и умения в нова или непозната среда. Те трябва да придобият умения за вземане на решения в сложни условия при влиянието на различни взаимодействащи си и трудно предвидими фактори, да притежават умения за работа в екип, да проявяват новаторство и творчески подход при решаване на нестандартни казуси и задачи, да умеят да се самоусъвършенстват и повишават своята квалификация. Не по-малко по важност е да могат да представят и защитават свои идеи и тèзи и да водят дискусии, да излагат компетентно и разбираемо идеи, проблеми и решения, да проявяват честност, професионална етика, толерантност, предприемчивост и гъвкавост, да носят отговорности, съответни на длъжностите, предвидени за тази образователна степен. Студентите получават необходимите теоретични знания и изследователски умения, които им позволяват да продължат образованието си за получаване на образователната и научна степен "доктор".

Образователни и професионални цели:

Целта на обучението по специалността „Киберсигурност и превенция на киберпрестъпления“ е да осигури високопрофесионална подготовка в една от най-актуалните и перспективните технически области, свързана с използването на информационни технологии за осигуряване и подпомагане на откриване на киберзаплахи и превенция на кибератаки.

Целта на общата теоретична подготовка е студентите да получат знания и умения на системни инженери, системни администратори, ръководители на проекти и други длъжности, свързани с разработването и прилагането на информационни системи в киберпространството. Тези специалисти трябва да имат абстрактно мислене, да могат да анализират процесите и да правят и предлагат технически решения и задания, което отговаря и на най-често поставяните от работодателите и бизнеса изисквания за компетентност. В процеса на обучение по програмата ще се систематизират знанията, относно правните аспекти на електронните доказателства, компютърните престъпления, разкриване и разследване на киберпрестъпления, видео и аудио анализ в криминалистиката, политиките за киберсигурност, различни способи за защита на уеб приложения както и основни политики при изграждане на информационни системи и мрежи. Обучението ще бъде проектно-ориентирано – подход, предназначен да даде на студентите възможност да развият знания и умения, чрез ангажиране в проекти около предизвикателства и проблеми, с които могат да се сблъскат в реалния свят и професионалното си развитие.

Целта на специалната подготовка по киберсигурност и превенция на кибератаки е да даде солидни знания, умения, навици, нагласи и ценности за проектиране, конструиране, имплементиране, тестване и поддържане на информационна сигурност, чрез противопоставяне на въздействия, засягащи наличието, истинността, целостта или поверителността на съхранявани, пренасяни или обработвани данни в информационни системи. Подготовката включва теми от областите на електронните доказателства, разкриване и разследване на киберпрестъпления, компютърна и мрежова сигурност, политики за киберсигурност, анализиране, разработване и аргументиране на решения за изграждане на системи за киберсигурност, умения за провеждане на научни изследвания и въвеждане на иновации.

Реализация на завършилите специалисти:

Магистрите по „Киберсигурност и превенция на киберпрестъпления“ ще бъдат подготвени да се реализират като специалисти, анализатори и консултанти по информационна сигурност, мениджъри и администратори по киберсигурност, експерти в разследването на кибератаки и в противодействието на киберзаплахи, кибератаки и киберкризи. Те могат да се реализират като разработчици на сигурен код и софтуер за киберсигурност, а също така като научни работници в изследователски организации и университети в областта на информационната сигурност. Обучението по специалността предоставя голяма адаптивност в пазарна среда, позволяваща поддържане на придобитите знания и умения в съответствие с бъдещото развитието на информационните технологии в областта на киберсигурността.

Пазарната ниша и изискванията на бизнеса предоставят потенциал за реализация на завършили студенти с такава специалност. Завършилите специалността магистри ще имат знания и умения за работа на разнообразни професионални позиции в държавни и правителствени агенции, частни финансови институции и други организации и фирми у нас и в чужбина, които се стремят да засилят защитата си срещу киберзаплахи с използване на компютърни технологии за осигуряване и поддържане на информационна сигурност.