Специалност: **Киберсигурност**
Код по ЕСТК: **BCS**

Образователно-квалификационна степен: бакалавър-инженер по Киберсигурност

Форма на обучение: редовно

Срок на обучение: 4 години

Завършване: с дипломен проект

Прием: на общо основание, съгласно действащия Правилник на ТУ – София, обучението по специалността се провежда на българскии език

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

Актуалност:

Целта на обучението по специалност „Киберсигурност“ съответства на мисията, визията, ценностите и стратегията за развитие на Технически университет – София. Основната образователна цел на специалността е да осигури подготовка на високо професионално ниво в една от най-актуалните и най-перспективните технически области, свързана с използването на компютърни и комуникационни технологии за подпомагане и осигуряване на киберсигурността. Едно от най-ценните богатства в света, в който живеем, изпълнен с дигитални технологии, е изобилието от информация. Предизвикателство към всеки специалист е тя да бъде надеждно защитена от непозволен достъп, от непозволено използване или разкриване, от прекъсване, промяна или унищожаване. Осигуряването на киберсигурността е многостепенен процес за управление на риска, който включва разпознаването на уязвимости, източници на заплаха и осигуряването на контрол. Дигитализацията ще продължи да се развива с бурни темпове и да навлиза все повече в живота, а едновременно с това ще растат сложността и разнообразието на опитите за непозволен достъп до информация, както и мерките за възпирането им. Този процес обуславя и тенденцията за нарастващо търсене на специалисти по киберсигурност.

Обща характеристика на обучението:

За успешната професионална дейност на бакалавър-инженера по „Киберсигурност“ е необходимо придобиването на теоретични знания и разбиране на основните факти, понятия, термини и теории в областта на компютърните системи и софтуерните технологии, а също и умения за прилагането на тези знания за проектиране, програмиране, реализиране, поддържане, развитие, адаптиране и локализиране на компютърни и информационни системи. За да се постигне по-голям обхват и мобилност на завършилите бакалаври и за да се осигури по-широко поле за бъдеща професионална изява се дава акцент на класическото знание, което да осигури високо ниво на разбиране на теоретичните основи на изучаваните дисциплини, а също и реализацията им в практиката. Бакалавър-инженерът по „Киберсигурност“ трябва да бъде с висока професионална подготовка и с богата езикова култура, както и с познания в областта на икономиката, мениджмънта, маркетинга, предприемачеството.

Образователни и професионални цели:

Специфичната цел на специалността е да даде солидни знания, умения, навици, нагласи и ценности за проектиране, конструиране, имплементиране, тестване и поддържане на мрежова и информационна сигурност чрез противопоставяне на въздействия, засягащи отрицателно наличието, истинността, целостта или поверителността на съхранявани, пренасяни или обработвани данни в комуникационни и компютърни мрежи и информационни системи. Поради изключително динамичните темпове на развитие на компютърните технологии и свързаните с това нарастващи заплахи, инженерите по киберсигурност трябва да поддържат нивото на придобитите знания и умения в съответствие с иновационните постижения и нови технологии в областта. Една от целите на обучението в специалността е да създаде у студентите мотивация за непрестанно надскачане на уменията, знанията и творческото мислене.

Фундаменталната подготовка се осъществява през първите четири семестъра от обучението чрез изучаване на курсове за придобиване на фундаментални знания в областта на математика, физика, инженерно проектиране, материалознание, електротехника, полупроводникови елементи,

механични системи, компютърни системи, сигнали и системи, измервания в информационните и комуникационни технологии, базови програмни езици, платформено-независими програмни езици, синтез и анализ на алгоритми, основи на мрежовите технологии, бази данни, чужди езици.

Специалната подготовка включва изучаването на задължителни академични курсове в областите основи на предаване на информация, мрежова сигурност, сигурност на физичния слой в безжичните комуникации, сигурност на операционни системи, обектно-ориентирано програмиране, криптографски методи за защита на информацията, глобални бази данни, софтуерни платформи, биометрични системи, сигурни архитектури и протоколи за комуникация, сигурност в безжични мрежи, етично хакерство. Профилиращата подготовка на бакалавър- инженерите предвижда изучаването на избираеми академични курсове в два модула: "Софтуерни приложения с повишена сигурност" и „Комуникационна и мрежова сигурност". Избираемите дисциплини обхващат областите сигурно системно програмиране, защита на web приложения, разпределени приложения и защита, машинно обучение и киберсигурност, програмни технологии за сигурен код, валидация и верификация на програмни системи, блокчейн технологии, сигурност и защита в Интернет на нещата за модул „Софтуерни приложения с повишена сигурност" и сигурност в киберфизични системи, надеждност и безопасност в критични инфраструктури, системи за видеонаблюдение, машинно обучение и дълбоки невронни мрежи с приложения в мрежовата сигурност, стеганография, видео и аудио анализ в криминалистиката, блокчейн в телекомуникациите, одит и оптимизация на мрежи за модул „Комуникационна и мрежова сигурност". Съобразно интересите си студентите могат да изберат за изучаване курсове в областите системи с изкуствен интелект и киберсигурност, квантови комуникации и квантова криптография, приложна криптография, сигурност в EDGE базирани IoT мрежи, както и курсове за придобиване на икономически и мениджърски познания и компетенции: анализ и управление на риска, управление на киберсигурността, теория и практика на ЕС в областта на киберсигурността, дигитален маркетинг, антикризисен мениджмънт в киберсигурността, мениджмънт на високите технологии. Факултативните курсове дават възможност на студентите да разширят познанията си в хуманитарната и правната области като изберат за допълнително изучаване професионално ориентиране в киберсигурността, стандарти за киберсигурност, политики за сигурност и прилагане, изследвания и анализ на дигитално съдържание, правни аспекти на киберсигурността, защита на интелектуалната собственост.

Реализация на завършилите специалисти:

Завършилите специалността бакалавър-инженери 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 и комуникационни технологии за осигуряване и поддържане на информационна сигурност. Бакалавър-инженерите по „Киберсигурност" са подготвени да се реализират като специалисти, анализатори и консултанти по информационна и комуникационна сигурност, мениджъри и администратори по киберсигурност, 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 и комуникационните технологии в областта на киберсигурността.