KONSTANTIN
PRESLAVSKY
UNIVERSITY
S H U M E N

ШУМЕНСКИ УНИВЕРСИТЕТ
"ЕПИСКОП КОНСТАНТИН ПРЕСЛАВСКИ"

гр. Шумен 9700, ул."Университетска" № 115
www.shu.bg

Ректор 054/ 830 350, факс 054/ 830 371
e-mail: rector@shu.bg

Утвърдил
Декан:
.....
проф. д-р Х. Христов

ФАКУЛТЕТ ПО ТЕХНИЧЕСКИ НАУКИ

КВАЛИФИКАЦИОННА ХАРАКТЕРИСТИКА

За специалност „ТЕХНОЛОГИИ ЗА КИБЕРСИГУРНОСТ"

Област на висше образование: 5. Технически науки
Професионално направление: 5.3 Комуникационна и компютърна техника
Образователно-квалификационна степен: Бакалавър
Професионална квалификация: Инженер по технологии за киберсигурност

Квалификационната характеристика на специалността „Технологии за киберсигурност" с образователно-квалификационна степен „Бакалавър", както и учебният план, осигуряващ подготовката, са съобразени с изискванията на Закона за висшето образование, Наредбата за държавните изисквания за придобиване на висше образование на образователно-квалификационните степени „бакалавър", „магистър" и „специалист", Европейската система за натрупване и трансфер на кредити във висшите училища, Европейската квалификационна рамка за учене през целия живот, Правилник за устройството и дейността на ШУ, Правилник за структурата и организацията на учебния процес в ШУ.

1. Цели на специалността

Бакалавърската програма „Технологии за киберсигурност" има за цел да подготвя висококвалифицирани технически кадри със задълбочена подготовка във всички фундаментални аспекти на мрежовата и информационна сигурност, които да осигурят противодействие на различни видове кибератаки и опити за неоторизиран достъп до информационните ресурси в държавни институции, частни фирми и организации, както и доставчици и потребители на цифрови услуги.

Основната цел определя насочеността на обучението на студентите в образователно-квалификационна степен „Бакалавър", специалност „Технологии за киберсигурност" към:

- придобиване на знания и умения за проектиране, експлоатация и поддръжка на комуникационна и компютърна техника и технологии.

- придобиване на знания за основните проблеми и методите за тяхното решаване, отнасящи се до мрежовата и информационната сигурност, до процесите при реагиране и управление на инциденти в киберпространството, както и придобиване и прилагане на умения за откриване на уязвимости в компютърните мрежи и системи.

- подготовка за изпълнение на професионалните задължения в съвременното информационно общество, чрез придобиване на необходимата инженерна и комуникативна култура;

- запознаване със световно утвърдените принципи на етичното хакерство.

- натрупване на личен опит, съответстващ на професионалната дейност на бъдещия инженер по защита на комуникационните и информационните ресурси в съвременните мрежови и информационни системи от различни видове кибератаки.

- формиране на компетенции за бърза адаптация към най-новите достижения в техническите и програмните средства за противодействие на различни видове киберзаплахи.

- придобиване на задълбочени знания за кибератаката за получаване на информационни отпечатъци и прилагане на разузнавателни техники, както и начини за нейното противодействие.

- придобиване на задълбочени знания за сканиращите мрежови техники, както и за начините за тяхното противодействие.

- придобиване на задълбочени знания за информационните системни кибератаки, както и за начините за тяхното противодействие.

В резултат на обучението по специалността „Технологии за киберсигурност" се получават следните резултати, отговарящи на квалификацията за образователно-квалификационна степен „Бакалавър":

- **за знания**: специализирани и теоретични знания в рамките на определената сфера на работа (Киберсигурност) и осъзнаване на границите на тези знания;

- **за умения**: богат диапазон от познавателни и практически умения, необходими за разработване на творчески решения на абстрактни проблеми;

- **за компетентност** (в контекста на Квалификационната рамка на Европейското пространство за висше образование компетентността се описва с оглед на степента на поемане на отговорност и самостоятелност): упражняване на управление и наблюдение в контекста на работни дейности, при които съществуват непредвидими промени, преглед и развитие на собствените постижения и постиженията на другите.

2. Квалификационен стандарт – компетенции на завършилите ОКС „Бакалавър" студенти.

Обучението на бъдещите инженери по специалността „Технологии за киберсигурност" е насочено към формиране на интелектуално-познавателна, мотивационно-ценностна, педагого-комуникативна и действено-практическа компетентност. Общите компетенции се развиват през целия период на обучение на студента. Базовите компетенции се придобиват през цикъла, в който студентът получава инженерна подготовка по направление Комуникационна и компютърна техника, а специфичните – в края на четиригодишния период на обучение.

2.1. Област и обхват на знанията.

Завършилите образователно-квалификационна степен „Бакалавър" по специалността „Технологии за киберсигурност" следва да притежават интердисциплинарни знания за:

- основните положения на линейната алгебра, аналитичната геометрия, от диференциалното и интегрално смятане на функции, на реални и комплексни променливи, от теорията на вероятностите, математическата статистика и случайните процеси;

- същността на физическите процеси, протичащи в линейни електрически вериги при постоянен и при променлив ток;
- устройството и принципите на работа на приборите за измерване на електрически величини;
- аритметичните и логически основи на компютърните системи;
- устройството, принципите на действие на аналоговите и цифрови схеми със средна и голяма степен на интеграция и тяхното използване в съвременните технически системи за сигурност;
- принципите и методите за предаване на данни между мрежовите възли, както и стандартите за изграждане на компютърни мрежи;
- архитектурата и програмирането на микропроцесорни системи и на микроконтролери;
- принципите на изграждане на компютърните архитектури и интерфейси, а така също и системното и програмното им осигуряване;
- цифровата обработка на сигналите, видовете модулации и произтичащите от тях особености при изграждането на различните технически устройства (преносна среда, , средства за защита на информацията, периферия и др.);
- използването на съвременни компютърни технологии за проектиране и синтез на аналогови и цифрови устройства;
- структурата и принципите на работа на специализираните радиоприемници, методите за определяне местоположението на източниците на сигнали, специализираните технически устройства, използвани за сриване на работата на системи за подслушване, възможностите на широколентовите технологии за изграждане на системи за сигурност с висока надеждност;
- методите за алгоритмизация и съставяне на програми на алгоритмичен език от високо ниво;
- принципите на приложение на математическите основи на киберсигурността;
- начините на изграждане, поддържане и администриране на компютърна и мрежова сигурност;
- начините на администриране на Windows базирани операционни системи;
- начините на администриране на Unix и Linux базирани операционни системи;
- начините на прилагане и изграждане на политики на сигурност в операционните системи;
- структурата и принципа на проектиране и програмиране на бази от данни;
- основите на мениджмънта на системите за сигурност и способите за оптимизиране на решенията и управлението на риска в киберсигурността;
- методите за противодействие на съвременни видове кибератаки, насочени към информационните ресурси на компютърните мрежи и системи;
- начините на изграждане и поддържане на системите за виртуализация;
- средствата и принципите на програмиране и сигурност мобилни устройства;
- начините на тестване на компютърни системи и мрежи за уязвимости;
- принципите и методите на защита на WEB базирани приложения;
- структурата и начина на създаване и приложение на софтуерни хибридни защитни стени, системи за известяване и предотвратяване на злонамерени проникванията в информационните ресурси на хостовете в компютърните мрежи и системи;
- начините и методите на криптиране на предаваната информация в компютърните мрежи и системи;

- принципите и начините на писане на сигурен код.

2.2. Област и обхват на компетенциите и уменията.

2.2.1. Лични компетенции и умения.

1. Комуникативни умения на роден език:

- да се изразяват и анализират мисли, чувства и факти в устна и писмена форма (слушане, говорене, четене и писане);

- да се общува в подходяща форма в разнообразен социален и културен контекст - образование и обучение, в работата, у дома и в свободното време.

2. Комуникативни умения на чужд език: способността да се разбират, изразяват и тълкуват мисли, чувства и факти в устна и писмена форма (слушане, говорене, четене и писане) в разнообразен социален контекст - на работа, у дома, в свободното време, по време на обучение - според индивидуалните нужди на чужд език.

3. Поддържане на широка осведоменост за новостите в областта на мрежовата и информационна сигурност.

4. Развиване на аналитично и конструктивно и мислене при изграждане на защитни мрежови механизми.

5. Използване на специализирани хардуерни и софтуерни инструменти за мрежово сканиране на хостове.

6. Развиване на умения за преодоляване на нови киберзаплахи от тип нулев ден.

7. Формиране на професионална мотивираност и отношение към бъдещата професия като етичен хакер.

8. Създаване на умения за поддържане на професионални взаимоотношения, изградени на основата на общи интереси за работа в екип.

9. Изграждане на умение за по-нататъшно самообучение и самоусъвършенстване при работа със софтуерни хибридни защитни стени.

10. Формиране на култура за общуване и спазване на общочовешките ценности и етичните норми.

11. Способност за изграждане на план и за определяне на цели, които да бъдат постигнати.

2.2.2. Професионални компетенции и умения.

1. Математическа грамотност и базови познания в областта на техническите науки и информационната сигурност в т.ч. способност и желание да се използват съществуващи знания и методология с цел да се даде обяснение на заобикалящата ни природа и физични закони; разбиране и приложение на знания и методологии с оглед на желанието и необходимостта.

2. Дигитални компетентности в т.ч. логично и точно мислене, обработване на голям обем от информация; употребата на мултимедийни технологии с цел да се извлича, оценява, съхранява, създава, представя и обменя информация.

3. Умения за самостоятелно учене и събиране, анализ и използване на информация.

4. Аналитичност.

5. Умение за прилагане на знанията в практиката.

6. Умение да се учи на място, където се работи.

7. Умение за работа в екип (сътрудничество, взаимодействие) в т.ч. способност да се представят идеи и да се изслушват внимателно идеите на другите; разбиране на динамиката на комуникацията и проследяване на съдържанието ѝ; умение да се конструира устойчива връзка чрез тактичност; способност да се вземат решения, които включват различни гледни точки.

8. Умение за формулиране на проблеми, свързани с работата.

9. Умение за предлагане на решения на поставени проблеми.

10. Умение за работа в среда на стандартизирани писмени инструкции, правила и процедури.

11. Умение за адаптиране при промяна на ситуацията.

13. Изследователски умения.

14. Мотивираност за бърза кариера и значим успех.

Специфични компетенции:

1. Да умеят да работят с нормативната уредба в сферата на киберсигурността.

2. Да изграждат и поддържат локални компютърни мрежи.

3. Да разработват политика за мрежова и информационна сигурност.

4. Да анализират и оценят риска от инциденти в киберсигурността.

5. Да извършват тестове с цел защита на информационните ресурси от загуба на конфиденциалност, интегритет и достъпност.

6. Да филтрират мрежовия трафик в локалната компютърна мрежа по IPv4/IPv6 логически мрежов адрес, по номер на порт, по име на услуга, по мрежово състояние и др.

7. Да използват криптографски механизми с цел осигуряване на конфиденциалност и интегритет на конфиденциалната информация.

8. Да изграждат и поддържат виртуални частни мрежи.

9. Да прилагат стриктни мерки и механизми за защита от проникване и средства за откриване и защита от зловреден софтуер в комуникационните мрежи и системи.

10. Да осигуряват физическа защита на информационните ресурси чрез прилагане на адекватни мерки и механизми срещу заплахи от неоторизиран физически достъп.

11. Да анализират и открият аномалии при предаването на информационни потоци, протоколи и файлове в компютърната мрежа чрез използването на хардуерни мрежови сензори и софтуерни инструменти за следене и мониторинг на трафика.

12. Да извършват контрол и одит на комуникационни и информационни системи.

13. Да проектират планове за прекъсваемост на комуникационната инфраструктура в случай на природни бедствия, аварии или други форсмажорни обстоятелства.

14. Да анализират физическите процеси, протичащи в линейни и нелинейни, електрически и магнитни вериги.

15. Да работят със специализирана комуникационна техника за определяне местоположението на източниците на сигнали.

16. Да умеят да решават задачи, свързани с проектиране, конфигуриране, настройката и експлоатацията на техническите системи за охрана, видеонаблюдение, пожароизвестяване и контрол на достъпа.

17. Да използват специализирани технически устройства за сриване на работата на системи за подслушване, възможностите на широколентовите технологии за изграждане на системи за сигурност с висока надеждност.

18. Да използват съвременни методи за обработка на звуков сигнал и видеоизображение в програмна среда Matlab, Labview и Fastcap при работа на системите за видеонаблюдение, системите за контрол на достъпа и в системите за идентификация и разпознаване на стационарни и динамични обекти.

19. Да организират информационната закрила и противодействието на различните посегателства при функционирането на организациите.

20. Да извършват тестове за познати и нови уязвимости в операционни системи, приложен специализиран софтуер и локални, градски и глобални компютърни мрежи.

21. Да използват съвременните бази от данни за най-новите появили се уязвимости в киберпространството.

22. Да противодействат на кибератаките от тип социално инженерство.

23. Да противодействат на кибератаките с отказ на услуги.

24. Да противодействат на кибератаките с откradване на сесия.

25. Да противодействат на кибератаките, насочени към уеб сървъри и уеб приложения.

26. Да противодействат на кибератаките с компютърни червеи и вируси.

27. Да противодействат на кибератаките с „троянски кон“ и „задна врата“.

28. Да осигуряват спазването на професионалните стандарти за етично хакерство.

3. Възможности за реализация.

Завършилите специалността „Технологии за киберсигурност” са подготвени да работят като:

- Служители в Отдел „Киберсигурност“ при Главна дирекция „Борба с организираната престъпност” в секторите „Кибератаки и онлайн хазарт“, „Противоправно съдържание в интернет“ и „Дигитални анализи и открити източници“.
- Експерти във държавната администрация, финансови, застрахователни и други институции с предмет на дейност защита на личните данни чрез прилагане на Регламента за общата защита на данните (GDPR).
- специалисти по сигурността на информационните и комуникационните технологии в техническите звена на институциите от сектора за сигурност - ДАНС, ДАТО, ДАР, МО, МВР, ГД „Охрана“ към Министерство на правосъдието, Служба Военна полиция и др.
- системни администратори, софтуерни разработчици, както и системни анализатори с предмет на дейност осигуряване на мрежова и информационна сигурност в държавни институции, частни фирми и организации.
- Консултанти и експерти по компютърни престъпления в международни асоциации, институти и неправителствени организации по информационна сигурност като (ISC)², SANS, ISACA, MITRE, CERT, EC-Council, Offensive Security, OWASP Foundation и др.
- Вещи лица и експерти с предмет на дейност изготвяне на съдебни инженерно-технически експертизи в Районните и Окръжни прокуратури, както и в Районните и Окръжни съдилища в Република България.
- преподаватели във висши училища в Република България и чужбина.

4. Изисквания за придобиване на ОКС „Бакалавър” по специалността „Технологии за киберсигурност”.

Образователно - квалификационната степен „Бакалавър“ се придобива в рамките на четири учебни години (осем семестъра и 240 кредита) в редовна форма на обучение, съгласно приложения Учебен план. Дипломирането се осъществява в два варианта:

Първи вариант: Държавен изпит – писмен;

Втори вариант: Защита на дипломната работа.

Дипломираните се получават професионална квалификация „Инженер по технологии за киберсигурност“.

До разработка на дипломна работа се допускат студенти с успех, не по-нисък от „Много добър“ (4,50) от всички семестриални изпити.

5. Възможности за допълнителна квалификация.

Придобилите образователно-квалификационна степен “Бакалавър” по специалността „Технологии за киберсигурност” имат възможност да продължат обучението си за получаване на ОКС “Магистър” по специалност от професионални направления

„Комуникационна и компютърна техника" и „Национална сигурност", а след това да се обучават за получаване и на образователната и научна степен "доктор".