ХАРАКТЕРИСТИКА НА УЧЕБНАТА ДИСЦИПЛИНА

Наименование на учебната дисциплина: **Сигурност в безжични мрежи**	Код: **BCS15**	Семестър: **7**
Вид на обучението: Лекции (Л), Лабораторни упражнения (ЛУ) Курсова работа (КР) - по избор	Семестриален хорариум: Л – 30 часа, ЛУ – 30 часа	Брой кредити: **5**
Курсов проект (КП) - по избор	Код: **BCS21**	Брой кредити: **2**

ЛЕКТОРИ:
доц. д-р инж. Георги Балабанов (ФТК), тел.: 965 34 56, email: grb@tu-sofia.bg
доц. д-р инж. Росен Милетиев (ФТК), тел.: 965 20 82, e-mail: miletiev@tu-sofia.bg
Технически университет-София

СТАТУТ НА ДИСЦИПЛИНАТА В УЧЕБНИЯ ПЛАН: Задължителна учебна дисциплина от учебния план за обучение на студенти за ОКС „бакалавър“, специалност “Киберсигурност”, професионално направление 5.3 Комуникационна и компютърна техника, област 5. Технически науки.

ЦЕЛИ НА УЧЕБНАТА ДИСЦИПЛИНА: Целта на обучението е да се дадат на студентите в систематизиран вид задълбочени познания за сигурността в безжичните мрежи. Студентите, приключили обучението си, трябва да познават архитектурата на безжичните мрежи, политиките, стандартите и протоколите свързани със сигурността, възможните методи за атаки и мерките за тяхното предотвратяване.

ОПИСАНИЕ НА ДИСЦИПЛИНАТА: Основни теми: Въведение в безжичните мреж, Локални и глобални безжични мрежи, Клетъчни мобилни мрежи, Сензорни мрежи, Основни механизми за сигурност в безжични мрежи, Политики за сигурност в безжични мрежи, Предизвикателства пред сигурността на безжичните мрежи, Проблеми със сигурността и методи за защита на Wi-Fi мрежи, клетъчни мобилни мрежи, безжични M2M системи, безжични сензорни мрежи, Проблеми със сигурността и методи за защита в мобилни Ad Hoc мрежи, Проблеми със сигурността и методи за защита на мобилни устройства, Системни основи на сигурността и поверителност за безжични мрежи от следващо поколение.

ПРЕДПОСТАВКИ: Въведение в информационната сигурност, Мрежова сигурност, Архитектури и протоколи за мрежови комуникации с повишена сигурност.

МЕТОД ЗА ПРЕПОДАВАНЕ: Лекции с използване на слайдове, лабораторните упражнения с протоколи и курсова работа със защита

МЕТОДИ НА ИЗПИТВАНЕ И ОЦЕНЯВАНЕ: Писмен изпит (75 %), лабораторни упражнения (20%), курсова работа (5%).

ЕЗИК НА ПРЕПОДАВАНЕ: Български

ПРЕПОРЪЧИТЕЛНА ЛИТЕРАТУРА: 1. Shen Zhong, Hong Zhong. *Security and Privacy for Next-Generation Wireless Networks*, Springer, 2019. 2. Lee Badman, *CWSP® - Certified Wireless Security Professional*, Second edition, Certitrek Publishing, 2019 3. Osterhage W., *Wireless Network Security*. CRC Press. 2021. 4. Shafiullah K., Al-Sakib Pathan. *Wireless Networks and Security: Issues, Challenges and Research Trends*, Springer, 2013. 5. Lei Chen, Jiahuang Ji, *Wireless Network Security*, Springer, 2013. 6. В.Рамачандран, К.Бюканън, *Kali Linux – изследване и етично хакване на Wireless мрежи*, Асеневци, 2019.

ХАРАКТЕРИСТИКА НА УЧЕБНАТА ДИСЦИПЛИНА

Наименование на учебната дисциплина: **Етично хакерство**	Код:**BCS16**	Семестър: **7**
Вид на обучението: Лекции (Л) Лабораторни упражнения (ЛУ) Курсова работа (КР) –по избор	Семестриален хорариум: Л – 30 часа ЛУ – 30 часа	Брой кредити: **5**
Курсов проект (КП) –по избор	Код: **BCS21**	Брой кредити: **2**

ЛЕКТОР(И):
Проф. д-р Даниела Гоцева (ФКСТ), тел.: 029652338, e-mail: dgoceva@tu-sofia.bg
ас. инж. Костадин Панчев (ФКСТ), e-mail: kpanchev@tu-sofia.bg
Технически университет-София

СТАТУТ НА ДИСЦИПЛИНАТА В УЧЕБНИЯ ПЛАН: Задължителна учебна дисциплина от учебния план за обучение на студенти за ОКС „бакалавър“, специалност “Киберсигурност“ професионално направление 5.3 Комуникационна и компютърна техника, област 5. Технически науки.

ЦЕЛИ НА УЧЕБНАТА ДИСЦИПЛИНА: Целта на учебната дисциплина е студентите да изучат различни хакерски инструменти, методи за провеждане на атаки, анализ на приложения за наличие на технологични пропуски и да придобият знания, свързани с проктирането, изграждането и поддръжката на сигурността на информационните и комуникационни системи.

ОПИСАНИЕ НА ДИСЦИПЛИНАТА: Основни теми: Въведение в етичното хакерство; Анализ и атаки на приложения; „Shellcode“; “Metasploit”; Сканиране за технологични пропуски; Атаки към пароли; Атаки, насочени към каналното ниво на OSI модела; Атаки на безжични мрежи; Атаки на WEB сървъри и WEB приложения; Подслушване на мрежови трафик и генериране на пакети; Заобикаляне на пароли при Microsoft Windows; Атаки на бази данни и инжектиране на SQL; Атаки на мобилни устройства с Android и т.н.

ПРЕДПОСТАВКИ: Изискват се познания по програмни езици, операционни системи, програмни среди, системно и WEB програмиране.

МЕТОД ЗА ПРЕПОДАВАНЕ: Лекции с използване на проектор, видео презентация и демо-програми, лабораторните и семинарни упражнения се провеждат в специализирани лаборатории.

МЕТОДИ НА ИЗПИТВАНЕ И ОЦЕНЯВАНЕ: Две двучасови контролни в средата и края на семестъра.

ЕЗИК НА ПРЕПОДАВАНЕ: български/английски

ПРЕПОРЪЧИТЕЛНА ЛИТЕРАТУРА: 1. Abraham K White, Hacking: The Underground Guide to Computer Hacking; 2. Daniel Regalado, Shon Harris, Allen Harper, Gray Hat Hacking: The Ethical Hacker's Handbook, Fifth Edition 5th Edition; 3. Александър Цокев, Етично хакерство,2017.

ХАРАКТЕРИСТИКА НА УЧЕБНАТА ДИСЦИПЛИНА

Наименование на учебната дисциплина: **Разпределени приложения и защита**	Код: **BCS17.1**	Семестър: **7**
Вид на обучението: Лекции (Л) Семинарни упражнения (СУ) Лабораторни упражнения (ЛУ) Курсова работа (КР) – по избор	Семестриален хорариум: Л – 30 часа СУ – 15 часа ЛУ – 15 часа	Брой кредити: **5**
Курсов проект (КП) – по избор	Код: **BCS21**	Брой кредити: **2**

ЛЕКТОР(И):
Доц. д-р инж. Надежда Ангелова (ФКСТ), тел.: 965 2017, e-mail: n_angelova@tu-sofia.bg
Технически университет-София

СТАТУТ НА ДИСЦИПЛИНАТА В УЧЕБНИЯ ПЛАН: Свободноизбираема дисциплина от учебния план/учебните планове за обучение на студенти за ОКС „бакалавър“, специалност “Киберсигурност”, професионално направление 5.3 Комуникационна и компютърна техника, област 5. Технически науки.

ЦЕЛИ НА УЧЕБНАТА ДИСЦИПЛИНА: Основната цел на дисциплината е да създаде у студентите умения за изграждане на приложения с многослойна архитектура базирана на уеб/rest услуги и компонентно програмиране. Изграждане на защита на приложенията. Създаване на защитени услуги, както и на софтуерни клиенти, които да комуникират с услугите, чрез протоколи за обмен на информация, платформено независими. Умения за проектиране на нови архитектури, както и решения за извършване на миграции на платформи в нова среда.

ОПИСАНИЕ НА ДИСЦИПЛИНАТА: Основни теми: Развитие на програмирането в разпределени среди, видове архитектури и компонентно програмиране. Сигурност в разпределена среда. Съвременни технологии, платформена независимост на комуникации. Уеб и Rest услуги – изграждане, защита и употреба, XML технологии за обмени и съхранение на данни, видове парсери, JSON, SOA - архитектури базирани на услуги, микроуслуги. Бизнес процеси, основни принципи и проектиране на защитени архитектури.

ПРЕДПОСТАВКИ: Добро познаване на език за програмиране, както и програмна среда за разработка на софтуерни приложения. Познания по бази данни, мрежи , видове web решения и приложения.

МЕТОД ЗА ПРЕПОДАВАНЕ: Лекции с използване на слайдове и демо-програми, лабораторните упражнения и курсова работа с описание и защита.

МЕТОДИ НА ИЗПИТВАНЕ И ОЦЕНЯВАНЕ: Писмен изпит - 90 мин. – състоящ се от два теоритични въпроса (60%) и казус/задача (40%) (общо 100%), лабораторни упражнения (0%), курсова работа (0%). Оценката се формира само от изпита, курсовата работа е само за заверяване на семестъра, както и упражненията.

ЕЗИК НА ПРЕПОДАВАНЕ: български/английски

ПРЕПОРЪЧИТЕЛНА ЛИТЕРАТУРА: Web Services, Service-Oriented Architectures, and Cloud Computing, Second Edition: The Savvy Manager's Guide (... by Douglas K. Barry (Jan 24, 2013); RESTful Web APIs by Leonard Richardson, Mike Amundsen and Sam Ruby (Sep 30, 2013) JavaScript and JSON Essentials by Sai Srinivas Sriparasa (Oct 24, 2013); Beginning XML, 5th Edition by Joe Fawcett, Danny Ayers and Liam R. E. Quin (Jul 10, 2012).

ХАРАКТЕРИСТИКА НА УЧЕБНАТА ДИСЦИПЛИНА

Наименование на учебната дисциплина: **Системи за видеонаблюдение**	Код: **BCS17.2**	Семестър: **7**
Вид на обучението: Лекции (Л) Семинарни упражнения (СУ) Лабораторни упражнения (ЛУ) Курсова работа (КР) – по избор	Семестриален хорариум: Л – 30 часа СУ – 15 часа ЛУ – 15 часа	Брой кредити: **5**
Курсов проект (КП) – по избор	Код: **BCS21**	Брой кредити: **2**

ЛЕКТОР(И):

Доц. д-р инж. Иво Драганов (ФТК), тел.: 965 2274, e-mail: idraganov@tu-sofia.bg
Доц. д-р инж. Лиляна Дочева (ФТК), тел.: 965 3277, e-mail: docheva@tu-sofia.bg
Технически университет-София

СТАТУТ НА ДИСЦИПЛИНАТА В УЧЕБНИЯ ПЛАН: Задължително избираема учебна дисциплина от учебния план за обучение на студенти за ОКС „бакалавър“, специалност “Киберсигурност”, професионално направление 5.3 Комуникационна и компютърна техника, област 5. Технически науки.

ЦЕЛИ НА УЧЕБНАТА ДИСЦИПЛИНА: След завършване на курса студентите трябва да могат да прилагат методите и средствата за проектиране на системи за видеонаблюдение. Необходимо е също така студентите да могат да анализират структурата и начина на действие на вече изградени системи от този тип с възможност за тяхното обновяване и разширяване.

ОПИСАНИЕ НА ДИСЦИПЛИНАТА: Основни теми: Еволюция на системите за видеонаблюдение; Компоненти за изграждане на връзка при предаване на видео; Мрежови видеокамери; Технологии за производство на видеокамери; Термокамери; Технологии за видеокомпресия; Видеотранскодери; Способи за обмен на видео в разпределена среда; Сървъри за поточно предаване на видео; Сървъри за съхранение на видео; Управление на видео предаването; Услуги за видео съхранение; Интелигентни алгоритми за анализ на видео наблюдавани сцени; Принципи и етапи на изграждане на системи за видеонаблюдение; Оценка на качеството на работата на системи за видео наблюдение; Интегриране в единни системи за физическа сигурност; Защита на личната неприкосновеност при системите за видеонаблюдение.

ПРЕДПОСТАВКИ: Сигнали и системи, Компютърни системи, Измервания в информационните и комуникационните технологии, Основи на мрежовите технологии, Програмни езици, Програмни среди.

МЕТОД ЗА ПРЕПОДАВАНЕ: Лекции с използване на слайдове, лабораторните упражнения с протоколи и курсова работа с описание и защита.

МЕТОДИ НА ИЗПИТВАНЕ И ОЦЕНЯВАНЕ: Изпит по време на редовна сесия с продължителност 2 академични часа с отговори на отворен тип въпроси и решаване на задачи (100%).

ЕЗИК НА ПРЕПОДАВАНЕ: български

ПРЕПОРЪЧИТЕЛНА ЛИТЕРАТУРА: 1. Kolekar, M. H., Intelligent Video Surveillance Systems: An Algorithmic Approach, Chapman and Hall/CRC, 2018. 2. Blokdyk, G., Video Surveillance: A Complete Guide, 5StarCooks, 2019. 3. Neves, A., Intelligent Video Surveillance, Intechopen, 2019. 4. Moreira, R., A Survey on Video Surveillance Systems, LAP Lambert, 2017. 5. Thottempudi, P., Novel Approach for Detection of Objects in Surveillance Videos, LAP Lambert, 2017

ХАРАКТЕРИСТИКА НА УЧЕБНАТА ДИСЦИПЛИНА

Наименование на учебната дисциплина: **Машинно обучение и киберсигурност**	Код: **BCS18.1**	Семестър: **7**
Вид на обучението: Лекции (Л) Лабораторни упражнения (ЛУ) Курсова работа (КР) – по избор	Семестриален хорариум: Л – 30 часа ЛУ – 15 часа	Брой кредити: **5**
Курсов проект (КП) – по избор	Код: **BCS21**	Брой кредити: **2**

ЛЕКТОР(И):
Проф. д-р инж. Милена Лазарова (ФКСТ), тел.: 965 3285, e-mail: milaz@tu-sofia.bg
Гл. ас. д-р инж. Ралица Райнова (ФКСТ), тел.: 965 3054, e-mail: ralitza.raynova@tu-sofia.bg
Технически университет-София

СТАТУТ НА ДИСЦИПЛИНАТА В УЧЕБНИЯ ПЛАН: Задължително избираема учебна дисциплина от учебния план за обучение на студенти за ОКС „бакалавър“, специалност “Киберсигурност”, професионално направление 5.3 Комуникационна и компютърна техника, област 5. Технически науки.

ЦЕЛИ НА УЧЕБНАТА ДИСЦИПЛИНА: След завършване на курса студентите трябва да познават методите за машинно обучение, да имат умения за практическо моделиране и използване на машинно обучение за решаване на различни приложни задачи в областта на киберсигурността.

ОПИСАНИЕ НА ДИСЦИПЛИНАТА: Основни теми: Същност на машинното обучение, цели и приложения. Алгоритми за управляемо и неуправляемо обучение. Генеративни и дискриминативни подходи за машинно обучение. Статистически методи за обучение. Линейни методи за класификация. Класификация чрез най-близки съседи. Линейни методи за класификация чрез регресия. Машинно обучение с нелинейна регресия. Класификация чрез метод на опорни вектори. Машинно обучение с класификационни дървета. Машинно обучение чрез клъстеризация. Клъстеризация чрез k-means и йерархична клъстеризация. Машинно обучение с невронни мрежи. Обучение и самообучение при невронни мрежи. Конволюционни невронни мрежи. Дълбоко обучение. Обучаващи и тестови данни. Оценка на точността на алгоритмите за машинно обучение. Оценка на моделите след обучение. Неодостатъчно обучение и пре-обучение. Приложение на машинно обучение за киберсигурност.

ПРЕДПОСТАВКИ: Математика I, Математика II, Въведение в програмирането, Базови програмни езици, Платформено-независими програмни езици, Обектно-ориентирано програмиране.

МЕТОД ЗА ПРЕПОДАВАНЕ: Лекции с използване на проектор и видеопрезентация, лабораторни упражнения за създаване, анализ и дискусии на конкретни примери, курсова работа с описание и защита.

МЕТОДИ НА ИЗПИТВАНЕ И ОЦЕНЯВАНЕ: Изпит с отговори на теоретични въпроси, казуси и задачи в два академични часа (80%), оценка от изпълнение на индивидуални задачи, разработвани по време лабораторни упражнения (20%).

ЕЗИК НА ПРЕПОДАВАНЕ: български

ПРЕПОРЪЧИТЕЛНА ЛИТЕРАТУРА:
1. Andrew Ng, Machine Learning Yearning, https://www.deeplearning.ai/machine-learning-yearning; 2. Shalev-Shwartz S. and Ben-David S., Understanding Machine Learning: From Theory to Algorithms, Cambridge University Press, 2014; 3. Hearty J., Advanced Machine Learning with Python, PACK publishing, 2016; 4. Richert W. and Coelho L. P., Building Machine Learning Systems with Python, Packt Publishing, 2013; 5. Witten I. H., Frank E., Hall M. A., Data Mining: Practical Machine Learning Tools and Techniques, Morgan Kaufmann, 2011.

ХАРАКТЕРИСТИКА НА УЧЕБНАТА ДИСЦИПЛИНА

Наименование на учебната дисциплина: **Машинно обучение и дълбоки невронни мрежи с приложения в мрежовата сигурност**	Код: **BCS18.2**	Семестър: **7**
Вид на обучението: Лекции (Л) Лабораторни (ЛУ) Курсова работа (КР) – по избор	Семестриален хорариум: Л – 30 часа ЛУ – 15 часа	Брой кредити: **5**
Курсов проект (КП) – по избор	Код: **BCS21**	Брой кредити: **2**

ЛЕКТОРИ: Проф. д-р инж. Ивайло Атанасов (ФТК), тел.: 965 2050, e-mail: iia@tu-sofia.bg
Доц. д-р инж. Венцислав Трифонов (ФТК), тел.: 965 2134, e-mail: vgt@tu-sofia.bg
доц. д-р Агата Манолова ФТК, тел:029652274, е-мейл: amanolova@tu-sofia.bg
гл. ас. д-р Никол Христова, ФТК, тел:02 9652274, е-мейл: nicole.christoff@tu-sofia.bg
Технически университет-София

СТАТУТ НА ДИСЦИПЛИНАТА В УЧЕБНИЯ ПЛАН: Задължително избираема учебна дисциплина от учебния план за обучение на студенти за ОКС „бакалавър“, специалност “Киберсигурност”, професионално направление 5.3 Комуникационна и компютърна техника, област 5. Технически науки.

ЦЕЛИ НА УЧЕБНАТА ДИСЦИПЛИНА: Целта на учебната дисциплина е да предостави необходимите знания за използване на алгоритми за машинно обучение и архитектури на дълбоки невронни мрежи за решаване на големите проблеми, които съществуват в областта на киберсигурността. Дисциплината се фокусира върху изграждането на нови и ефективни решения, които да заменят традиционните механизми за киберсигурност и използването на колекция от алгоритми и архитектури, които увеличават сигурността на системите чрез автоматизация.

ОПИСАНИЕ НА ДИСЦИПЛИНАТА: Дисциплината запознава с основните етапи от жизнения цикъл на заплахите и начини за внедряване на интелигентни решения за киберсигурност. Обхванатa е теорията и практически приложения, оформени в контекста на реални сценарии за сигурност. Включени са примери за решаване на проблеми от реалния свят с помощта на алгоритми за машинно обучение като клъстеризиране, k-средни, линейна регресия и Naive Bayes. Ще се представят най-актуалните архитектури на дълбоки невронни мрежи като Рекурентни невронни мрежи и такива с дългосрочна памет за решаване на проблеми свързани с анализ на поведението на потребителите, анализ на текст за детекция на спам, откриване и предотвратяване на проникванията;

ПРЕДПОСТАВКИ: Въведение в програмирането, Математика I, II, III, Сигнали и системи, Бази данни; Мрежова сигурност; Биометрични системи.

МЕТОД ЗА ПРЕПОДАВАНЕ: Предвидени материали: презентации, видеа и допълващи файлове. На студентите се предоставя допълнителна литература и полезни линкове. За изпълнение на самостоятелните задачи, курсови работи или курсовия проект са разработени писмени указания, лабораторните и семинарните упражнения с протоколи.

МЕТОДИ НА ИЗПИТВАНЕ И ОЦЕНЯВАНЕ: Оценката се формира от следните компоненти: Изпит (67%) и 33% от самостоятелна работа, курсова работа, лаб. упражнения.

ЕЗИК НА ПРЕПОДАВАНЕ: български/английски

ПРЕПОРЪЧИТЕЛНА ЛИТЕРАТУРА: 1. S. Halder, S. Ozdemir. Hands-On Machine Learning for Cybersecurity, Packt Publishing, 2018, ISBN: 978-1788992282; 2. E. Tsukerman. Machine Learning for Cybersecurity Cookbook, Packt Publishing, 2019, ISBN: 978-1789614671; 3. M. Alazab, M. Tang, Deep Learning Applications for Cyber Security, Springer, 2019, ISBN: 9783030130572; 4. K. Kim, M. Aminanto, H. Tanuwidjaja, Network Intrusion Detection using Deep Learning: A Feature Learning Approach, Springer, 2018, ISBN: 9789811314445; 5. A. Parisi, Hands-On Artificial Intelligence for Cybersecurity: Implement smart AI systems for preventing cyber attacks and detecting threats and network anomalies. Packt Publishing Ltd, 2019, ISBN: 9781789805178.

ХАРАКТЕРИСТИКА НА УЧЕБНАТА ДИСЦИПЛИНА

Наименование на учебната дисциплина: **Изкуствен интелект и киберсигурност**	Код: **BCS19.1**	Семестър: **7**
Вид на обучението: Лекции (Л) Лабораторни упражнения (ЛУ) Курсова работа (КР) – по избор,	Семестриален хорариум: Л – 30 часа ЛУ – 15 часа	Брой кредити: **5**
Курсов проект (КП) – по избар	Код: **BCS21**	Брой кредити: **2**

ЛЕКТОР(И):

Проф. д-р инж. Румен Трифонов (ФКСТ), тел.: 965 2338, e-mail: r_trifonov@tu-sofia.bg
Технически университет-София

СТАТУТ НА ДИСЦИПЛИНАТА В УЧЕБНИЯ ПЛАН: Задължителна / свободноизбираема / задължително избираема / факултативна учебна дисциплина от учебния план/учебните планове за обучение на студенти за ОКС „бакалавър“, специалност “Киберсигурност”, професионално направление 5.3 Комуникационна и компютърна техника, област 5. Технически науки.

ЦЕЛИ НА УЧЕБНАТА ДИСЦИПЛИНА: Цел на дисциплината „Изкуствен интелект и киберсигурност“ е студентите да добият обща представа за системите с изкуствен интелект, да изучат и да могат да прилагат основните принципи на използването на теорията и методите на изкуствения интелект при киберсигурността, както и да получат практически навици в изследването и построяването на системи с изкуствен интелект за киберсигурност.

ОПИСАНИЕ НА ДИСЦИПЛИНАТА: Основни теми: Основи на изкуствения интелект: История, същност, основни термини и понятия в ИИ. Работа с данни и работа със знания. Инженерни задачи, решавани чрез прилагане на ИИ. Регресия. Клъстеризация. Модели за представяне на знанията“: Логически и мрежови модели за представяне на знанията. Продукционни модели. Фреймови модели. Семантични мрежи. Размита логика. Експертни системи – архитектура, етапи и технологии за построяване на експертни системи. Машинно обучение. Невронни мрежи. Алгоритми за обучение на невронни мрежи. Модел на Хопфилд. Модел на Кохонен. Рекурентни невронни мрежи. Оптимизация на дълбоки мрежи, Методи на изкуствения интелект за киберсигурност. Предвидените лабораторни упражнения способстват за осмисляне на лекционния материал и спомагат за формиране на практически умения.

ПРЕДПОСТАВКИ: „Програмни среди” и „Програмни езици“..

МЕТОД ЗА ПРЕПОДАВАНЕ: Лекции с използване на слайдове, лабораторни упражнения с демо програми и курсова работа с описание и защита.

МЕТОДИ НА ИЗПИТВАНЕ И ОЦЕНЯВАНЕ: Писмен изпит в края на семестъра (общо 65%), лабораторни упражнения (15%), курсова работа (20%).

ЕЗИК НА ПРЕПОДАВАНЕ: български

ПРЕПОРЪЧИТЕЛНА ЛИТЕРАТУРА: 1. Stuart Russell, Artificial Intelligence : A Modern Approach, 3Rd Edition, Pearson, 2015, 1164 p., ISBN-10 : 9789332543515; 2. Denis Rothman, Artificial Intelligence By Example: Develop machine intelligence from scratch using real artificial intelligence use cases, Packt Publishing, 2018, 490 p., ISBN-10 : 1788990544; 3. Владимир Йоцов. Изкуствен интелект и експертни системи, 2014, 4. Румен Трифонов, Г. Цочев, Методи на изкуствения интелект за мрежова и информационна

сигурност, Монография, изд. Авангард Прима, 2018, 168 стр., ISBN: 978-619-160-936-9; 5. Румен Трифонов и др., Мрежова и Информационна Сигурност, Авангард прима, 2013.

ХАРАКТЕРИСТИКА НА УЧЕБНАТА ДИСЦИПЛИНА

Наименование на учебната дисциплина: **Квантови комуникации и квантова криптография**	Код: **BCS19.2**	Семестър: **7**
Вид на обучението: Лекции (Л) Лабораторни упражнения (ЛУ) Курсова работа (КР) – по избор	Семестриален хорариум: Л – 30 часа ЛУ – 15 часа	Брой кредити: **5**
Курсов проект (КП) – по избор	Код: **BCS21**	Брой кредити: **2**

ЛЕКТОР(И):

Доц. д-р инж. Мария Ненова (ФТК), тел.: 965 21 34, e-mail: mvn@tu-sofia.bg

Доц. д-р инж. Кирил Късев (ФТК), тел.: 965 00 00, e-mail: kmk@tu-sofia.bg

Технически университет-София

СТАТУТ НА ДИСЦИПЛИНАТА В УЧЕБНИЯ ПЛАН: Задължителна учебна дисциплина от учебния план за обучение на студенти за ОКС „бакалавър“, специалност “КИБЕРСИГУРНОСТ”, професионално направление 5.3 Комуникационна и компютърна техника, област 5. Технически науки.

ЦЕЛИ НА УЧЕБНАТА ДИСЦИПЛИНА: След завършване на курса студентите трябва да могат да разбират принципите на работа на системите в киберпространството. Ще познават фундаменталните принципи на действие и структура на съвременните системи за квантово разпределение на криптографските ключове, концептуаленият и математически апарат, използван за доказване на стабилността на квантовите криптосистеми.

ОПИСАНИЕ НА ДИСЦИПЛИНАТА: По време на курса се изучават: Основи на квантова криптография и какви проблеми решава. Критерий на Шенън за абсолютна секретност. Математически основи на квантовата информатика. Описание на квантовите състояния на отделни и съставни квантови системи, чисти, смесени състояния, квантово заплитане, ортогонални и обобщени измервания, изчистване на квантови състояния, теорема за забрана за копиране, трансформации на квантови системи. Протоколи за квантовата комуникация и тяхното описание: квантова телепортация, свръхплътно кодиране, квантово разпределение на ключове. Протоколи за разпределение на квантови ключове: BB84, B92, E91, SARG04. Квантови комуникационни канали - честотна лента. Критерий за секретност на ключовете. Хеш-функции от втори ред, използвани в процедури за повишаване на секретността. Анализ на криптографската сигурност на реализации на квантови криптографски системи с неидеални източници на квантови състояния, детектори и квантов комуникационен канал със загуби. Квантови генератори на случайни числа. Атаки.

ПРЕДПОСТАВКИ: Математика, Въведение в програмирането, Операционни системи, Синтез и анализ на алгоритми, Компютърни системи, Основи на мрежовите технологии, Бази данни.

МЕТОД ЗА ПРЕПОДАВАНЕ: Лекции с използване на слайдове, симулатори и демо-програми, лабораторни упражнения с протоколи и курсов проект по проблеми, актуални за дисциплината.

МЕТОДИ НА ИЗПИТВАНЕ И ОЦЕНЯВАНЕ: Две едночасови писмени текущи оценки в средата и края на семестъра (общо 80%), лабораторни упражнения (20%).

ЕЗИК НА ПРЕПОДАВАНЕ: български

ПРЕПОРЪЧИТЕЛНА ЛИТЕРАТУРА:

1. Bennett, C.H., Bessette, F., Brassard, G. et al. Experimental quantum cryptography. J. Cryptology 5, https://doi.org/10.1007/BF00191318, 1992. 2. C.H. Bennet, " Quantum Cryptography Using Any Two Non-Orthogonal States", Phys. Rev. lett. 68, 3121 (1992). 3. Dilip Kumar Shaw, Kausik Saha, Quantum Key Distribution Scheme based on BB84 Protocol, LAP LAMBERT Academic Publishing, ISBN:6139999804, 2019. 4. Gerardus Blokdyk, Quantum Computing A Complete Guide - 2020 Edition, ISBN: 0655924965, 5STARCooks, 2021. 5. Nirbhay Kumar Chaubey and Bhavesh B. Prajapati, Quantum Cryptography and the Future of Cyber Security (Advances in Information Security, Privacy, and Ethics) 1st Edition, IGI Global, ISBN:1799822532, 2020. 6. Simon Edwards, Quantum Computing and Modern Cryptography 2 books in 1: A Complete Guide. Discover History, Features, Developments and Applications of New Quantum Computers and Secrets of Modern Cryptography, Independently published, ISBN: 979-8624095328, 2020.

ХАРАКТЕРИСТИКА НА УЧЕБНАТА ДИСЦИПЛИНА

Наименование на учебната дисциплина: **Анализ и управление на риска**	Код: **BCS20.1**	Семестър: **7**
Вид на обучението: Лекции (Л) Семинарни упражнения (СУ) Курсова работа (КР)	Семестриален хорариум: Л –30 часа СУ – 15 часа	Брой кредити: **3**

ЛЕКТОР(И):
Проф. д-р инж. Огнян Наков (ФКСТ), тел.: 965 2513, e-mail: nakov@tu-sofia.bg
Доц.. д-р инж. Върбинка Стефанова-Стоянова (ФКСТ), тел.: 965 3363, e-mail: vvstoyanova@tu-sofia.bg
Технически университет-София

СТАТУТ НА ДИСЦИПЛИНАТА В УЧЕБНИЯ ПЛАН: Избираема учебна дисциплинаот учебния план/учебните планове за обучение на студенти за ОКС „бакалавър“, специалност “Киберсигурност”, професионално направление 5.3 Комуникационна и компютърна техника, област 5. Технически науки.

ЦЕЛИ НА УЧЕБНАТА ДИСЦИПЛИНА: Цел на дисциплината „Анализ и управление на риска“ е да предостави на студентите практическо и научно-изследователско ноу-хау в сферата на анализа, оценката и управлението на риска в работните и съпътстващите процеси, с акцент върху значението и динамизма на бъдещата работна среда.

ОПИСАНИЕ НА ДИСЦИПЛИНАТА: Основни теми:Идентифициране на рисковете: Методи за оценка и идентификация на потенциални рискове и заплахи за информационните системи и мрежи.Анализ на риска: Детайлно проучване на методите за анализ на риска, включително квантитативен и качествен анализ, за да се определят потенциалните въздействия на различните заплахи.Управление на риска: Стратегии и процеси за управление на идентифицирани рискове, включително приемане, избягване, смекчаване и прехвърляне на риска. Планиране за възстановяване при бедствия и непредвидени ситуации.Преглед на основните международни и национални регулации и стандарти за киберсигурност, включително GDPR, ISO/IEC 27001 и NIST. Risk Management As A Service .

ПРЕДПОСТАВКИ: Информационни системи, управление, математически анализ, теория на вероятностите и математическа статистика, теоретични основи на компютърните науки, корпоративна архитектура, компютърни системи, мрежи, телекомуникации..

МЕТОД ЗА ПРЕПОДАВАНЕ: Лекциите се провеждат с помощта на мултимедиен проектор, като се излагат структурата на лекцията, основни определения, модели, формули, графики и фигури и алгоритми. Студентите могат предварително да получат достъп до лекционните материали.

МЕТОДИ НА ИЗПИТВАНЕ И ОЦЕНЯВАНЕ: Две едночасови писмени контролни работи в средата и края на семестъра (общо 80%) и семинарни упражнения (20%).

ЕЗИК НА ПРЕПОДАВАНЕ: български

ПРЕПОРЪЧИТЕЛНА ЛИТЕРАТУРА: Risk Management Policy And Procedures, Version 4.0, GPE Risk Management Framework and Policy

ХАРАКТЕРИСТИКА НА УЧЕБНАТА ДИСЦИПЛИНА

Наименование на учебната дисциплина: **Управление на киберсигурността**	Код: **BCS20.2**	Семестър: **7**
Вид на обучението: Лекции (Л) Семинарни упражнения (СУ),	Семестриален хорариум: Л – 30 часа СУ – 15 часа	Брой кредити: **3**

ЛЕКТОР(И):

Проф. д-р инж. Румен Трифонов (ФКСТ), тел.: 965 2338, e-mail: r_trifonov@tu-sofia.bg
Технически университет-София

СТАТУТ НА ДИСЦИПЛИНАТА В УЧЕБНИЯ ПЛАН: Задължителна / свободноизбираема / задължително избираема / факултативна учебна дисциплина от учебния план/учебните планове за обучение на студенти за ОКС „бакалавър“, специалност “Киберсигурност”, професионално направление 5.3 Комуникационна и компютърна техника, област 5. Технически науки.

ЦЕЛИ НА УЧЕБНАТА ДИСЦИПЛИНА: Дисциплината “Управление на киберсигурността” има за цел запознаване на студентите с основните понятия, стандарти и техники в областта на управлението на мрежовата и информационна сигурност. Студентите ще се запознаят с нормативна база, която регулира дейността на българските структури на киберсигурност. Целта на курса е да създадат у студентите знания и умения, свързани с добрите практики при прилагането на съвременни методи за управление на системите за киберсигурността в компютърно-информационна инфраструктура.

ОПИСАНИЕ НА ДИСЦИПЛИНАТА: Курсът „Управление на киберсигурността“ представя основните направления на управление на киберсигурността в киберпространството. Киберсигурността обхваща защитата на системите, мрежите и данните във виртуалното пространство. Прави се въведение в областта с основните определения и ключовите характеристики в това направление. Представят се най-важните подходи, определянето на политиките на киберсигурност за автоматизираните информационни системи, стандарти и заплахи срещу мрежовата и информационна сигурност. Предвидените семинарни упражнения способстват за осмисляне на лекционния материал и спомагат за формиране на практически умения.

ПРЕДПОСТАВКИ: Основи на мрежовите технологии, Компютърни системи и Висша математика.

МЕТОД ЗА ПРЕПОДАВАНЕ: Лекции с използване на слайдове, семинарните упражнения със задачи и казуси за практическо решаване.

МЕТОДИ НА ИЗПИТВАНЕ И ОЦЕНЯВАНЕ: Писмен изпит в края на семестъра (общо 75%), семинарни упражнения (25%).

ЕЗИК НА ПРЕПОДАВАНЕ: български

ПРЕПОРЪЧИТЕЛНА ЛИТЕРАТУРА: 1. Сигурност и защита на информацията. Автор(и): Цветан Семерджиев Издателство: Софттрейд; 2012 г. ISBN: 9789543341382; 2. Румен Трифонов и др., Мрежова и Информационна Сигурност, Авангард прима, 2013; 3. http://www.enisa.europa.eu/.; 4. ISO/IEC 27032:2012, Information technology — Security techniques — Guidelines for cybersecurity; 5. https://www.paloaltonetworks.com/cyberpedia/what-is-cyber-security.

ХАРАКТЕРИСТИКА НА УЧЕБНАТА ДИСЦИПЛИНА

Наименование на учебната дисциплина: **Теория и практика на ЕС в областта на киберсигурността**	Код: **BCS 20.3**	Семестър: **7**
Вид на обучението: Лекции (Л) Семинарни упражнения (СУ)	Семестриален хорариум: Л – 30 часа СУ – 15 часа	Брой кредити: **3**

ЛЕКТОР(И):

Доц. д-р инж. Мария Ненова (ФТК), тел.: 965 21 34, e-mail: mvn@tu-sofia.bg
Доц. д-р инж. Кирил Късев (ФТК), тел.: 965 21 34, e-mail: kmk@tu-sofia.bg
Технически университет-София

СТАТУТ НА ДИСЦИПЛИНАТА В УЧЕБНИЯ ПЛАН: Избираема учебна дисциплина от учебния план за обучение на студенти за ОКС „бакалавър“, специалност “КИБЕРСИГУРНОСТ”, професионално направление 5.3 Комуникационна и компютърна техника, област 5. Технически науки.

ЦЕЛИ НА УЧЕБНАТА ДИСЦИПЛИНА: След завършване на курса студентите трябва да могат да разбират основните изисквания и принципите на работа на европейското законодателство и практическото му прилагане в областта на киберсигурността. Те ще знаят каква е регулаторната рамка и да я прилагат при реализацията на комуникационни и информационни системи.

ОПИСАНИЕ НА ДИСЦИПЛИНАТА: По време на курса се изучават: Основи на принципи на Киберсигурността, Действия на ЕС в областта на Киберсигурността, Регулаторни инструменти, политики и стратегии на НАТО и ЕС в областта на киберсигурността, Закон за киберсигурност, Стратегия за киберсигурност, Наредба за минималните изисквания за мрежова и информационна сигурност, Национална програма за Киберсигурност, Управление на сигурността в ЕС, Изисквания на НАТО и държавите членки, Обмен на информация и координация между държавите членки и ЕС, Защита на критичната инфраструктура и обществените функции в ЕС, Механизми за киберзащита в ЕС, Управление на оперативната съвместимост между страните членки на ЕС, Гарантиране на защитата на националните бази данни в ЕС, Център на НАТО за реагиране при инциденти с компютърната сигурност, Киберсигурност и приложение на иновативни технологии – принципи и изисквания, Европейска рамка за изграждане на сигурни системи.

ПРЕДПОСТАВКИ: Глобални бази данни, Криптографски методи за защита на информацията, Операционни системи, Компютърни системи, Основи на мрежовите технологии, Бази данни.

МЕТОД ЗА ПРЕПОДАВАНЕ: Лекции с използване на слайдове, симулатори и демо-програми, семинарни упражнения.

МЕТОДИ НА ИЗПИТВАНЕ И ОЦЕНЯВАНЕ: Две едночасови писмени текущи оценки в средата и края на семестъра (общо 80%), семинарни упражнения (20%).

ЕЗИК НА ПРЕПОДАВАНЕ: български

ПРЕПОРЪЧИТЕЛНА ЛИТЕРАТУРА:
1. The Art of Invisibility, Kevin Mitnick, Little, Brown and Company, ISBN-10 : 0316380504, 2017 2. Serious Cryptography: A Practical Introduction to Modern Encryption by Jean-Philippe Aumasson .ISBN-13: 978-1593278267, 2017 3. Defensive Security Handbook: Best Practices for Securing Infrastructure 1st Edition by Lee Brotherston, Amanda Berlin ISBN-13: 978-1491960387, 2017. 4. Jacob G. Oakley, Waging Cyber War: Technical Challenges and Operational Constraints, Apress, ISBN-10: 1484249496, 2019. 5. Blockchain for dummies,Tiana Laurence, ISBN-13 : 978-1119555018, 2019. 6. Jacob G. Oakley, Waging Cyber War: Technical Challenges and Operational Constraints, Apress, ISBN-10: 1484249496, 2019; 7. Закон за киберсигурност, „Държавен вестник“, 31.10.2018.

ХАРАКТЕРИСТИКА НА УЧЕБНАТА ДИСЦИПЛИНА

Наименование на учебната дисциплина: **Антикризисен мениджмънт в киберсигурността**	Код: **BCS20.4**	Семестър: **7**
Вид на обучението: Лекции (Л) Семинарни упражнения (СУ) Курсова работа (КР)	Семестриален хорариум: Л – 30 часа СУ – 15 часа	Брой кредити: **3**

ЛЕКТОР(И):
Проф. дн Минчо Христов Куминев, тел.: 965 2180, mincho-hristov@tu-sofia.bg
Ас.д-р Анна Пенкова (СФ), тел.: 965 2180, e-mail: a.penkova@tu-sofia.bg
Технически университет-София

СТАТУТ НА ДИСЦИПЛИНАТА В УЧЕБНИЯ ПЛАН: Избираема/ от учебния план/ за обучение на студенти за ОКС „бакалавър“, специалност “Киберсигурност”, професионално направление 5.3 Комуникационна и компютърна техника, област 5. Технически науки.

ЦЕЛИ НА УЧЕБНАТА ДИСЦИПЛИНА: **Целта на учебната дисциплина** е да запознае студентите с управлението на кризи в областта на сигурността. Обръща се внимание върху интересите, които биха могли умишлено да провокират кризи. Засегнати са начините на управление и противодействие на различни по своя характер природни, екологични, социални, военни, политически и други типове кризи, както и тяхната взаимовръзка. Разглеждат се основните методи за противодействие срещу кризите

ОПИСАНИЕ НА ДИСЦИПЛИНАТА: Основни теми на курса са: Причини, същност и типология на кризите. Същност и задачи на антикризисния мениджмънт. Конфликтологията като наука и методи за решаване на кризи. Видове кризи и основни последствия за обществото. Особености на националната сигурност. Технология при управлението на кризи – същност и специфика. Субекти и интереси при създаването на кризи. Политически кризи и тяхното управление. Мениджмънт на икономическите кризи. Социални кризи и тяхното предотвратяване. Глобални заплахи за сигурността. Роля на корпоративната сигурност. Киберсигурност и общество. Роля на специализираните държавни структури в управлението на сигурността. Специфика и характеристики на потенциални кризисни ситуации в България.

ПРЕДПОСТАВКИ: Теория на управлението, информатика, обществознание, право, история,

МЕТОД ЗА ПРЕПОДАВАНЕ: Лекции с използване на проектор и демо-програми.

МЕТОДИ НА ИЗПИТВАНЕ И ОЦЕНЯВАНЕ: курсова работа 50% и изпит 50%.

ЕЗИК НА ПРЕПОДАВАНЕ: български/

ПРЕПОРЪЧИТЕЛНА ЛИТЕРАТУРА: Рикардс, Д., След кризата, С., 2020; Христов, М., Аспекти на парламентаризма в системата на българската демокрация, С., 2018, Денчев, С.,Информация и сигурност, С.,2019;Начев, Й., Дълбоката държава, С., 2019;Harvard Business Essentials, Управление на кризи, прогнозиране и преодоляване, С. 2007; Фергюсън, Н., Пари и власт в модерния свят, С., 2020, Великов, И., Превенцията на кризи, С., 2010; Чангов, М., Процедури при анализ на конфликти и кризи, НСС – МВР, С., 2003; Христов, М., Глобалистика, С., 2018.

ХАРАКТЕРИСТИКА НА УЧЕБНАТА ДИСЦИПЛИНА

Наименование на учебната дисциплина: **Мениджмънт на високите технологии**	Код: **BCS20.5**	Семестър: **7**
Вид на обучението: Лекции (Л) Семинарни упражнения (СУ)	Семестриален хорариум: Л – 30 часа СУ – 15 часа	Брой кредити: **3**

ЛЕКТОР(И):
Доц. д-р инж. Борислав Иванов Николов (СФ), тел.: 965 3519, e-mail: bnikolov@tu-sofia.bg
Технически университет-София

СТАТУТ НА ДИСЦИПЛИНАТА В УЧЕБНИЯ ПЛАН: Свободноизбираема мениджърска учебна дисциплина от учебния план за обучение на студенти за ОКС „бакалавър“, специалност “Киберсигурност”, професионално направление 5.3 Комуникационна и компютърна техника, област 5. Технически науки.

ЦЕЛИ НА УЧЕБНАТА ДИСЦИПЛИНА: След завършване на курса студентите ще познават понятийния апарат на мениджмънта, ще могат да анализират различни мениджърски проблеми в областта на високите технологии и ще могат да вземат компетентни мениджърски решения.

ОПИСАНИЕ НА ДИСЦИПЛИНАТА: Основни теми: Вътрешна и външна среда на бизнес организациите. Развитие на теорията на управлението. Съвременни предизвикателства пред мениджмънта във високотехнологичните предприятия. Мениджмънт в “E-Business” среда. Управление на риска, Организационно проектиране на високотехнологичното предприятие. Мениджмънт на операциите във високотехнологичното предприятие. Мениджмънт на високотехнологични проекти, Мениджмънт на човешките ресурси и др.

ПРЕДПОСТАВКИ: Технологичен практикум, Висша математика и статистика, Основи на инженерното проектиране.

МЕТОД ЗА ПРЕПОДАВАНЕ: Лекциите се провеждат с помощта на преносим компютър и мултимедиен прожектор, чрез които на екран се проектира съпътстващият графичен материал: слайдове със схеми, диаграми, графики.

МЕТОДИ НА ИЗПИТВАНЕ И ОЦЕНЯВАНЕ: Писмен изпит (тест) в края на учебния семестър – определя 80% от крайната оценка. Самоподготовката и участието на студентите в хода на обучението се отчитат посредством показаните резултати при решаваните примери и конкретни проблеми, касаещи предварително зададена реална ситуация през семестъра – определят 20% от крайната оценка.

ЕЗИК НА ПРЕПОДАВАНЕ: български

ПРЕПОРЪЧИТЕЛНА ЛИТЕРАТУРА:
1. Андреев, О., Мениджмънт на проекти, Софттрейд, 2013.; 2. Даков, Организация на производствени и операционни системи, ТУ-София, 2015 г; 3. Николов Б., Управление на риска при реинженеринг на бизнес процесите, ИК „Кинг“, 2016; 4. Khalil T., Management of Technology: the key to competitiveness and wealth creation, McGraw-Hill Education Pvt Limited, 2009. 5. Pinto J.K. Project Management: Achieving Competitive Advantage, 5th ed., Pearson, 2019, ISBN 1292269146. 6. Sushil D., Cases in Strategic Management: A Flexibility Perspective, Springer, 2019, ISBN 978-9811370632, 981137063X.; 7. Kerzner H. Innovation Project Management: Methods, Case Studies, and Tools for Managing Innovation Projects, Wiley, 2019, ISBN 978-1-119-58729-3; 8. Olson D.L., Wu D.D. Enterprise Risk Management Models, 3rd ed. — Springer, 2020, ISBN 3662606070, 9783662606070, 9783662606087.

ХАРАКТЕРИСТИКА НА УЧЕБНАТА ДИСЦИПЛИНА

Наименование на учебната дисциплина: **Програмни технологии за сигурен код**	Код: **BCSE22.1**	Семестър: **8**
Вид на обучението: Лекции (Л) Лабораторни (ЛУ) Курсова работа (КР) – по избор	Семестриален хорариум: Л – 20 часа ЛУ – 20 часа	Брой кредити: **4**

ЛЕКТОР(И):

Проф. д-р инж. Огнян Наков Наков(ФКСТ), тел.: 965 3613, e-mail: nakov@tu-sofia.bg
Технически университет-София

СТАТУТ НА ДИСЦИПЛИНАТА В УЧЕБНИЯ ПЛАН: задължително избираема учебна дисциплина от учебния план за обучение на студенти за ОКС „бакалавър“, специалност “Киберсигурност”, професионално направление 5.3 Комуникационна и компютърна техника, област 5. Технически науки.

ЦЕЛИ НА УЧЕБНАТА ДИСЦИПЛИНА: студентите се запознават с техники и технологии за пробив на код, както и със софтуерните технологии и средства за създаване програмен код, устойчив на хакерски атаки и сривове.. В практическите занятия се запознават със среди за pen-тестиране и оценяване устойчивост на приложения от различен тип на хакерски атаки

ОПИСАНИЕ НА ДИСЦИПЛИНАТА: Основни теми: технологии, утилити и среди за сканиране и pen- тестиране (активно и пасивно). Вируси и макровируси. Троянски коне, warm атаки, социално инженерство. Атаки праз препълване, атаки към информационни системи, хакерски атаки в Internet, DoS атаки, атаки през Regular expressions, атаки през XML. Навсякъде се разглеждат софтуерни технологии и техники за противодействие.

ПРЕДПОСТАВКИ: синтез и анализ на алгоритми, Криптография, програмни езици, програмни среди

МЕТОД ЗА ПРЕПОДАВАНЕ: Лекции с използване на слайдове и демо-програми, лабораторните упражнения с протоколи и курсова работа за разработка на устойчив код или анализ стабилността на приложение с описание и защита.

МЕТОДИ НА ИЗПИТВАНЕ И ОЦЕНЯВАНЕ: писмен изпит, включващ 2 въпроса. Възможно е по задание на водещия преодавател да се разработи завършен проект и след защита и проверка ефективността на вложените в него технологии да се приравни на изпит.

ЕЗИК НА ПРЕПОДАВАНЕ: български/английски

ПРЕПОРЪЧИТЕЛНА ЛИТЕРАТУРА:

1.Хауърд М., Д. Лебланк, Писане на сигурен код, Microsoft Press, third edd, 2009;

2. Seacord R., Secure Coding in C and C++Pearson Edd, 2013

3. Stalling W., Computer Security - principle s and practice, Pearson, 2017

4. Peter Kin, The Hacker playbook, Secure planet LLC, 2016

5. Ehittacker J., How to break software security, Addison Wesley, 2008

6. Shostack Adam, Thread modelling, Wiley, 2018.

ХАРАКТЕРИСТИКА НА УЧЕБНАТА ДИСЦИПЛИНА

Наименование на учебната дисциплина: **Стеганография**	Код: **BCS22.2**	Семестър: **8**
Вид на обучението: Лекции (Л) Лабораторни упражнения (ЛУ) Курсова работа (КР) – по избор	Семестриален хорариум: Л – 20 часа ЛУ – 20 часа	Брой кредити: **4**

ЛЕКТОР(И):
Проф. д-р инж. Снежана Плешкова (ФТК), тел.: 965 2274, e-mail: snegpl@tu-sofia.bg
Доц. д-р инж. Румен Миронов (ФТК), тел.: 965 2274, e-mail: rmironov@tu-sofia.bg
Доц. д-р инж. Иво Драганов (ФТК), тел.: 965 2274, e-mail: idraganov@tu-sofia.bg
Технически университет-София

СТАТУТ НА ДИСЦИПЛИНАТА В УЧЕБНИЯ ПЛАН: Задължително избираема учебна дисциплина от учебния план за обучение на студенти за ОКС „бакалавър“, специалност “Киберсигурност”, професионално направление 5.3 Комуникационна и компютърна техника, област, 5. Технически науки.

ЦЕЛИ НА УЧЕБНАТА ДИСЦИПЛИНА: След завършване на курса студентите трябва да могат да прилагат основните подходи за скриване на информацията в текстови съобщения, изображения, видео и аудио, да познават програмните системи за моделиране и симулация (Octave, Phyton) и ги използват за решаване на конкретни инженерни задачи в областта на стеганографията.

ОПИСАНИЕ НА ДИСЦИПЛИНАТА: Основни теми: Основни принципи на стеганографията; сигурност в стеганографските системи; скриване на информацията в текстови съобщения, изображения, видео и аудио; методи за обработка във времевата и честотната област; статистически характеристики и анализ на информацията; методи за водно маркиране и защита на авторските права; основни изисквания към включваните водни знаци; видове атаки към водните знаци, защита и анализ.

ПРЕДПОСТАВКИ: Математика I, II, III. Базови програмни езици, Сигнали и системи, Бази данни, Платформено-независими програмни езици, Биометрични системи, Въведение в информационната сигурност

МЕТОД ЗА ПРЕПОДАВАНЕ: Лекции с използване на слайдове и демо-програми, лабораторните упражнения с протоколи.

МЕТОДИ НА ИЗПИТВАНЕ И ОЦЕНЯВАНЕ: Двучасов писмен изпит (общо 90%), лабораторни упражнения (10%).

ЕЗИК НА ПРЕПОДАВАНЕ: български

ПРЕПОРЪЧИТЕЛНА ЛИТЕРАТУРА: 1. Gerardus Blokdyk, Steganography, 3th Ed., 5STARCooks, 2019, ISBN-10: 0655532714, ISBN-13: 978-0655532712; 2. Sujatha Canavoy Narahari, Secure Transmission of Text through Images with Encryption Algorithms: Image Steganography. LAP LAMBERT Academic Publishing, 2017. ISBN-10: 6202071982, ISBN-13: 978-6202071987; 3. Ismael Abdul Sattar, Steganography In Spatial Domain. LAP LAMBERT Academic Publishing, 2018. ISBN-10: 6134955450, ISBN-13: 978-6134955454.

ХАРАКТЕРИСТИКА НА УЧЕБНАТА ДИСЦИПЛИНА

Наименование на учебната дисциплина: **Валидация и верификация на програмни системи**	Код: **BCS23.1**	Семестър: **8**
Вид на обучението: Лекции (Л) Лабораторни (ЛУ) Курсова работа (КР) – по избор	Семестриален хорариум: Л – 20 часа ЛУ – 20 часа	Брой кредити: **4**

ЛЕКТОР(И):
доц. д-р Аделина Алексиева-Петрова (ФКСТ),тел.: 965 26 52, email: aaleksieva@tu-sofia.bg
Технически университет-София

СТАТУТ НА ДИСЦИПЛИНАТА В УЧЕБНИЯ ПЛАН: Задължително избираема дисциплина за студенти, обучавани за получаването на образователно-квалификационна степен „бакалавър“ по специалност "Киберсигурност" във Факултет по компютърни системи и технологии, ТУ – София.

ЦЕЛИ НА УЧЕБНАТА ДИСЦИПЛИНА: Дисциплината запознава с целите, особеностите и спецификите на процесите на валидация и верификация на програмни системи. Основната насока на курса е към създаване на разбиране и умение за разпознаване на проблемите в разработваните програмни системи, определяне на начините за намаляване на възможностите за проява на дефекти в програмните системи, както и с някои аспекти на психологията на разработчиците, водещи до поява на дефекти в програмните среди. Дисциплината е приложно ориентирана, като всички теми са свързани с примери от конкретни проекти и програмни системи.

ОПИСАНИЕ НА ДИСЦИПЛИНАТА: Основните теми са свързани с: цели и задачи на процесите за валидация и верификация; изисквания за осигуряване на качеството и надеждността на разработваното програмно осигуряване, основни принципи и стратегии процесите на валидацията и верификация на програмно осигуряване; методи за верификация на програмно осигуряване; методи за валидация на програмно осигуряване; стандарти, средства и среди за реализация на етапите на валидация и верификация; модулното и интеграционното тестване; рефакторинг.

ПРЕДПОСТАВКИ: Изискват се познания по всички специални предмети, включващи проектиране, анализ и реализация на програмно осигуряване, както и предметите по софтуерно и системно инженерство.

МЕТОД ЗА ПРЕПОДАВАНЕ: Лекции с използване на слайдове и демо-програми, лабораторните упражнения и курсова работа с описание и защита.

МЕТОДИ НА ИЗПИТВАНЕ И ОЦЕНЯВАНЕ: Писмен (50%) и практичен (50%) изпит.

ЕЗИК НА ПРЕПОДАВАНЕ: български

ПРЕПОРЪЧИТЕЛНА ЛИТЕРАТУРА: 1. cs.tu-sofia.bg – електронен лекционен материал на А. Алексиева-Петрова; 2.Jorgensen, Paul C. Software testing: a craftsman’s approach. CRC press, 2018.; 3.Aristides Dasso, Ana Funes, Verification, Validation and Testing in Software Engineering, Idea Group Inc., 2007.; 4.B. Hambling (editor), Software Testing ISEB Foundation, BCS Publishing Products, 2009.; 5. A. Hunt, D. Thomas, Pragmatic Unit Testing in C# with NUnit, The Pragmatic Bookshelf, 3e, 2010; 6. W.L. Oberkampf, C.J. Roy, Verification and Validation in Scientific Computing, Cambridge University Press, 2010; 7. J. O. Grady, System Verification: Proving the Design Solution Satisfies the Requirements, Academic Press, 2010; 8. K. Lano, UML 2 Semantics and Applications, John Wiley & Sons, 2009.

ХАРАКТЕРИСТИКА НА УЧЕБНАТА ДИСЦИПЛИНА

Наименование на учебната дисциплина: **Видео и аудио анализ в криминалистиката**	Код: **BCS23.2**	Семестър: **8**
Вид на обучението: Лекции (Л) Лабораторни упражнения (ЛУ) Курсова работа (КР) – по избор	Семестриален хорариум: Л – 20 часа ЛУ – 20 часа	Брой кредити: **4**

ЛЕКТОР(И):
Проф. д-р инж. Снежана Плешкова (ФТК), тел.: 965 2274, e-mail: snegpl@tu-sofia.bg
Доц. д-р инж. Румен Миронов (ФТК), тел.: 965 2274, e-mail: rmironov@tu-sofia.bg
Доц. д-р инж. Иво Драганов (ФТК), тел.: 965 2274, e-mail: idraganov@tu-sofia.bg
Технически университет-София

СТАТУТ НА ДИСЦИПЛИНАТА В УЧЕБНИЯ ПЛАН: Задължително избираема учебна дисциплина от учебния план за обучение на студенти за ОКС „бакалавър“, специалност “Киберсигурност”, професионално направление 5.3 Комуникационна и компютърна техника, област, 5. Технически науки.

ЦЕЛИ НА УЧЕБНАТА ДИСЦИПЛИНА: След завършване на курса студентите трябва да могат да прилагат основните принципи и подходи за анализ на аудио и видео информация в криминалистиката, да познават програмните системи за анализ и обработка и да ги използват за решаване на конкретни инженерни задачи в областта на криминалистиката.

ОПИСАНИЕ НА ДИСЦИПЛИНАТА: Основни теми: Въведение в криминалистичния анализ, цифровизация, възпроизвеждане и анализ на видео и аудио, възстановяване на цифрово видео и аудио, възстановяване на файлове, процедури за обработка на видео и аудио доказателства, цифрова обработка на изображения, методология за аудио анализ, характеристики на речта и шума, принципи за изясняване на звука, гласова идентификация, идентификация на автора, фонетичен анализ, идентификация на говорителя, гласов спектрограф, инструменти и софтуер, използвани във видео и аудио анализа, анализ на снимки.

ПРЕДПОСТАВКИ: Математика I, II, III. Базови програмни езици, Сигнали и системи, Бази данни, Платформено-независими програмни езици, Биометрични системи, Въведение в информационната сигурност

МЕТОД ЗА ПРЕПОДАВАНЕ: Лекции с използване на слайдове и демо-програми, лабораторните упражнения с протоколи.

МЕТОДИ НА ИЗПИТВАНЕ И ОЦЕНЯВАНЕ: Двучасов писмен изпит (общо 90%), лабораторни упражнения (10%).

ЕЗИК НА ПРЕПОДАВАНЕ: български

ПРЕПОРЪЧИТЕЛНА ЛИТЕРАТУРА: 1. Joakim Kävrestad, Fundamentals of Digital Forensics: Theory, Methods, and Real-Life Applications, Springer; 2nd Ed., 2020. ISBN-10: 3030389537, ISBN-13: 978-3030389536.; 2. Robert C. Maher, Principles of Forensic Audio Analysis, Springer, 2018. ISBN-13: 978-3319994529, ISBN-10: 3319994522; 3. Forensic Video Analysis: A Complete Guide, The Art of Service - Forensic Video Analysis Publishing, 2021. ISBN-10: 1867412705, ISBN-13: 978-1867412700; 4. André Årnes, Digital Forensics, Wiley, 2017. ISBN-13: 978-1119262381, ISBN-10: 1119262380.

ХАРАКТЕРИСТИКА НА УЧЕБНАТА ДИСЦИПЛИНА

Наименование на учебната дисциплина: **Блокчейн технологии**	Код: **BCSE24.1**	Семестър: **8**
Вид на обучението: Лекции (Л) Лабораторни/семинарни упражнения (ЛУ/СУ) Курсова работа (КР) – по избор,	Семестриален хорариум: Л – 20 часа ЛУ – 20 часа	Брой кредити: **4**

ЛЕКТОР(И):

Гл. ас. д-р инж. Явор Томов (ФКСТ), тел.: 965 2606, email: yavor_tomov@tu-sofia.
Технически университет-София

СТАТУТ НА ДИСЦИПЛИНАТА В УЧЕБНИЯ ПЛАН: Задължително избираема дисциплина от учебния план за обучение на студенти по специалност “Киберсигурност ”, на Факултет ФКСТ на Технически Университет – София за образователно-квалификационна степен “бакалавър”.

ЦЕЛИ НА УЧЕБНАТА ДИСЦИПЛИНА: Дисциплината има за цел да запознае студентите с въпроси, на които се основават блокчейн технологиите, различните видове архитектури, алгоритмите за постигане на консенсусни модели, какво представляват криптовалутите и различните децентрализирани проекти.

ОПИСАНИЕ НА ДИСЦИПЛИНАТА: Разглеждат се основните разлики на децентрализираните системи с централизираните такива. Последователно се разглеждат криптографски методи и математически модели и алгоритми, които са пряко свързани с проблемите, които възникват при изграждането на една децентрализирана система, условията на който тя трябва да отговаря и различните видове консенсусни алгоритми. Отделя се внимание на въпросите, отнасящи се към сигурността на една такава система. Разглеждат се механизмите на работа на цифровите валути, техните имплементации и проекти, базирани на блокчейн технологията. Отделя се особено внимане и на интелигентните договори, които са една нова парадигма, върху която се строи нов вид дигитална индустрия. Разглеждат се програмни езици, чрез които могат да се реализират интелигентни договори. Разглеждат се и аспектите на сигурния код в интелигентните договори.

ПРЕДПОСТАВКИ: Предполага се, че студентите имат практически знания по програмни езици, структури от данни, криптографски базови знания, както и от мрежи.

МЕТОД ЗА ПРЕПОДАВАНЕ: Лекции, изнасяни с помощта на презентации и медиен проектор, както и предоставяне и обсъждане на допълнителен текстов материал за дисциплината. Лабораторни упражнения, изпълнявани по теми от лекциите под ръководство на преподавател, като основната задача на упражненията е да се разработи един пълноценен проект, базиран на блокчейн технологията.

МЕТОДИ НА ИЗПИТВАНЕ И ОЦЕНЯВАНЕ: Текуща оценка – две конролни работи (по една в средата и края на семестъра).

ЕЗИК НА ПРЕПОДАВАНЕ: български

ПРЕПОРЪЧИТЕЛНА ЛИТЕРАТУРА: 1. Mastering Blockchain: Distributed ledger technology, decentralization, and smart contracts explained August 2020 Edition: 3rd Pack ISBN: 978-1839213199 2. Mastering Ethereum: Building Smart Contracts and DApps 1st Edition by Andreas M. Antonopoulos (Author), Gavin Wood Ph. D. (Author) Publisher : O'Reilly Media; 1st edition (December 23, 2018) ISBN-13: 978-1491971949 3. Mastering Bitcoin: Programming the Open Blockchain 2nd Edition by Andreas M. Antonopoulos (Author) Publisher : O'Reilly Media; 2nd edition (July 11, 2017) ISBN-13 : 978-1491954386 3. The Bitcoin Standard: The Decentralized Alternative to Central Banking Hardcover – Illustrated, by Saifedean Ammous (Author) Publisher : Wiley; 1st edition (April 24, 2018) ISBN-13 : 978-1119473862.

ХАРАКТЕРИСТИКА НА УЧЕБНАТА ДИСЦИПЛИНА

Наименование на учебната дисциплина: **Блокчейн в телекомуникациите**	Код: **BCS24.2**	Семестър: **8**
Вид на обучението: Лекции (Л), Лабораторни упражнения (ЛУ) Курсова работа (КР) – по избор	Семестриален хорариум: Л – 20 часа, ЛУ – 20 часа	Брой кредити: **4**

ЛЕКТОРИ:
проф. д-р инж. Георги Илиев (ФТК), тел.: 965 30 29, email: gli@tu-sofia.bg
доц. д-р инж. Камелия Николова (ФТК), тел.: 965 21 34, email: ksi@tu-sofia.bg
Технически университет-София

СТАТУТ НА ДИСЦИПЛИНАТА В УЧЕБНИЯ ПЛАН: Избираема учебна дисциплина от учебния план за обучение на студенти за ОКС „бакалавър“, специалност “Киберсигурност”, професионално направление 5.3 Комуникационна и компютърна техника, област 5. Технически науки.

ЦЕЛИ НА УЧЕБНАТА ДИСЦИПЛИНА: Целта на обучението е да се дадат на студентите в систематизиран вид задълбочени познания в областта на блокчейн технологиите. Особено внимание се обръща на приложението на блокчейн системите в телекомуникациите и възможностите, които те предоставят за подобряване на тяхната сигурност. Студентите, приключили обучението си, трябва да познават основните принципи на работа на блокчейн системите, основните етапи от развитието на блокчейн технологиите, основните приложения на блокчейн системите свързани със сигурността в телекомуникационните мрежи, както и методите за атаки и мерките за тяхното предотвратяване.

ОПИСАНИЕ НА ДИСЦИПЛИНАТА: Основни теми: Основни елементи на блокчейн системите. Етапи в развитието на блокчейн технологиите. Механизми за консенсус. Смарт контракти. Кибер заплахи при блокчейн системите. Основни категории слабости, свързани с мрежата и алгоритмите за работа. Приложение на блокчейн технологиите в IoT мрежите за повишаване на сигурността и поверителността на информацията. Предизвикателства и приложения на Блокчейн базирани решения за облачни комуникации (Fog-RAN, IoT Edge). Блокчейн базирани SDN и виртуализация. Приложение на блокчейн в мобилните и безжичните мрежи. Блокчейн базирани платформи за DNS сигурност. Блокчейн базирана защита от DDoS атаки.

ПРЕДПОСТАВКИ: Въведение в информационната сигурност, Мрежова сигурност, Сигурност в безжични мрежи.

МЕТОД ЗА ПРЕПОДАВАНЕ: Лекции с използване на слайдове, лабораторните упражнения с протоколи.

МЕТОДИ НА ИЗПИТВАНЕ И ОЦЕНЯВАНЕ: Изпит (80%), Лабораторни упражнения (20%)

ЕЗИК НА ПРЕПОДАВАНЕ: Български

ПРЕПОРЪЧИТЕЛНА ЛИТЕРАТУРА:

1. S. K. Panda, A. K. Jena, S. K. Swain, S. C. Satapathy (Editors), Blockchain Technology: Applications and Challenges, Springer, 2021. 2. M. H. Rehmani, Blockchain Systems and Communication Networks: From Concepts to Implementation, Textbooks in Telecommunication Engineering, Springer, 2021. 3. M. M. Rehan, M. H. Rehmani (Editors), Blockchain-enabled Fog and Edge Computing: Concepts, Architectures, and Applications, CRC Press, 2021.

ХАРАКТЕРИСТИКА НА УЧЕБНАТА ДИСЦИПЛИНА

Наименование на учебната дисциплина: **Сигурност и защита в Интернет на нещата**	Код: **BCS25.1**	Семестър: **8**
Вид на обучението: Лекции (Л) Семинарни упражнения (СУ) Лабораторни упражнения (ЛУ) Курсова работа (КР) – по избор,	Семестриален хорариум: Л – 20 часа СУ – 10 часа ЛУ – 10 часа	Брой кредити: **4**

ЛЕКТОР(И):

проф. д-р Даниела Гоцева, (ФКСТ), тел.: 965 2338, e-mail: dgoceva@tu-sofia.bg
Технически университет-София

СТАТУТ НА ДИСЦИПЛИНАТА В УЧЕБНИЯ ПЛАН: Избираема дисциплина за редовни студенти по специалност “Киберсигурност” във Факултета по Компютърни системи и технологии на ТУ-София за образователно-квалификационна степен “бакалавър”.

ЦЕЛИ НА УЧЕБНАТА ДИСЦИПЛИНА: Основната цел на курса е студентите да придобият знания в областта на сигурност и защита в Интернет на нещата и да получат практически умения за защита на поверителността на данните, видове атаки и мерките за противодействие.

ОПИСАНИЕ НА ДИСЦИПЛИНАТА: Дисциплината предоставя в систематизиран и компресиран вид теоретични и практически знания и стратегии в областта на сигурност и защита в Интернет на нещата: malware схеми в Интернет на нещата, анализ на атаки върху Smart Home Systems, защита на поверителността, разпространение на SPG-базирани данни подобряване поверителността чрез алгоритъм за разпределени цветове, подобряване наличността чрез репликация на съобщения, заплахи и подходи за защита поверителността в smart сгради. В курса се застъпва още: модели за защита поверителността в приложения от Интернет на нещата.

ПРЕДПОСТАВКИ: Компютърни мрежи, Криптография, Бази данни.

МЕТОД ЗА ПРЕПОДАВАНЕ: Лекции, изнасяни с мултимедийни средства и лабораторни упражнения, с които се прилага и затвърдява лекционния материал.

МЕТОДИ НА ИЗПИТВАНЕ И ОЦЕНЯВАНЕ: Писмен изпит и текущ контрол през семестъра с компютърни тестове през електронната платформа за обучение и индивидуални задания.

ЕЗИК НА ПРЕПОДАВАНЕ: Български

ПРЕПОРЪЧИТЕЛНА ЛИТЕРАТУРА:
1. Shivani Agarwal, Sandhya Makkar, Duc-Tan Tran, Privacy Vulnerabilities and Data Security Challenges in the IoT, CRC Press, 2021. 2. Sudhir Sharma, Bharat Bhushan, Narayan Debnath, Security and Privacy Issues in IoT Devices and Sensor Networks, Elsevier, 2021. 3. Damilare D. Fagbemi, David M Wheeler, JC Wheeler, The IoT Architect's Guide to Attainable Security and Privacy, CRC Press, 2020. 4. Chintan Patel, Nishant Doshi, Internet of Things Security Challenges, Advances, and Analytics, CRC Press, 2019..

ХАРАКТЕРИСТИКА НА УЧЕБНАТА ДИСЦИПЛИНА

Наименование на учебната дисциплина: **Одит и оптимизация на мрежи**	Код: **BCS25.2**	Семестър: **8**
Вид на обучението: Лекции (Л) Семинарни упражнения (СУ) Лабораторни упражнения (ЛУ) Курсова работа (КР) – по избор	Семестриален хорариум: Л – 20 часа СУ – 10 часа ЛУ – 10 часа	Брой кредити: **4**

ЛЕКТОР(И):
доц. д-р инж. Златка Вълкова-Джарвис (ФТК), тел.: 965 3251, e-mail: zvv@tu-sofia.bg
доц. д-р инж. Бончо Бонев (ФТК), тел.: 965 3279, e-mail: bbonev@tu-sofia.bg
Технически университет-София

СТАТУТ НА ДИСЦИПЛИНАТА В УЧЕБНИЯ ПЛАН: Задължително избираема учебна дисциплина от учебния план за обучение на студенти за ОКС „бакалавър“, специалност “Киберсигурност”, професионално направление 5.3 Комуникационна и компютърна техника, 5. Технически науки.

ЦЕЛИ НА УЧЕБНАТА ДИСЦИПЛИНА: Целта на обучението е да се дадат на студентите знания по процесите на мониторинг, анализ, одит и оптимизация на комуникационните мрежи, за да се осигури тяхното оптимално и сигурно функциониране, съгласно установените стандарти. След завършване на курса студентите трябва да познават елементите на процеса на одит на мрежата, техническите способи за осъществяването им, да идентифицират проблемните области, да извършат анализ на състоянието и да предложат план за оптимизация на мрежата.

ОПИСАНИЕ НА ДИСЦИПЛИНАТА: Модул „*Одит на мрежи*“: Същност, необходимост, етапи на процеса на одит на мрежи. Преглед на основни мрежови компоненти и параметри и изготвяне на одитен доклад. Одит на преносна мрежа – координати и горещи аларми, мрежова конфигурация, преносни среди и захранване, антени и тестване на заземяване. Одит на радио мрежа – проверка на покритие, вътреклетъчен и междуклетъчен хендоувър, качество и мощност на сигналите в приемната страна, интерференция, успешни, блокирани и отхвърлени повиквания, услуги. Одит на базови станции и други комуникационни системи в мрежата – проверка на: BoQ (Bill of Quality), хардуерни и софтуерни аларми, връзките на RF коаксиални кабели и загуба на мощност. QoS (Quality of Services) сравнителен анализ и QoE (Quality of Experience) одит. Модул „ *Оптимизация на мрежи*“: Същност и етапи на оптимизацията на мрежи за гарантиране на сигурна комуникация. Оптимизация на радио мрежи (LTE, 5G) – трафик, прогнозирана мобилност на абонатите и тенденция за генериране на трафик за оптимално покритие и капацитет на мрежата, KPI (Key Performance Indicators) оптимизация. Методи за оптимизиране на преносната мрежа - оптимизационен модел на трафика, мрежовата топология, честотен план.

ПРЕДПОСТАВКИ: Основи на мрежовите технологии, Мрежова сигурност, Архитектури и протоколи за мрежови комуникации с повишена сигурност, Сигурност в безжични мрежи.

МЕТОД ЗА ПРЕПОДАВАНЕ: Лекции с използване на слайдове и демо-програми, лабораторните упражнения с протоколи и курсова работа с описание и защита.

МЕТОДИ НА ИЗПИТВАНЕ И ОЦЕНЯВАНЕ: Две писмени текущи оценки в средата и края на семестъра (общо 60%), лаб. и семинарни упражнения (20%), курсова работа (20%).

ЕЗИК НА ПРЕПОДАВАНЕ: български

ПРЕПОРЪЧИТЕЛНА ЛИТЕРАТУРА:
1. Chris Jackson. Network Security Auditing, Cisco Press, 2010, ISBN 978-1-58705-352-8; 2. M. S. Mastel, Telecom Audit, 2003, McGraw-Hill, ISBN: 9780071410540; 3. Christodoulos A. Floudas, Panos M. Pardalos, Encyclopedia of Optimization, Springer, 2009, ISBN: 978-0-387-74760-6.

ХАРАКТЕРИСТИКА НА УЧЕБНАТА ДИСЦИПЛИНА

Наименование на учебната дисциплина: **Приложна криптография**	Код: **BCS26.1**	Семестър: **8**
Вид на обучението: Лекции (Л) Семинарни упражнения (СУ) Лабораторни упражнения (ЛУ) Курсова работа (КР) – по избор	Семестриален хорариум: Л – 20 часа СУ –10 часа ЛУ – 10 часа	Брой кредити: **4**

ЛЕКТОР(И):

Доц. д-р инж. Антония Ташева (ФКСТ), тел.: 965 2224, e-mail: atasheva@tu-sofia.bg
Технически университет-София

СТАТУТ НА ДИСЦИПЛИНАТА В УЧЕБНИЯ ПЛАН: Свободно избираема учебна дисциплина от учебния план за обучение на студенти за ОКС „бакалавър“, специалност “Киберсигурност”, професионално направление 5.3 Комуникационна и компютърна техника, област 5. Технически науки.

ЦЕЛИ НА УЧЕБНАТА ДИСЦИПЛИНА: Дисциплината е проектно-ориентирана и цели студентите да усвоят практически умения по изграждане на сигурни софтуерни продукти, като прилагат съвременните алгоритми, методи и принципи на Криптографията. Добрите познания на нивата на криптографска защита могат да бъдат използвани в практиката на инженерите по киберсигурност както за проектиране и създаване, така и за проверка и повишаване на сигурността на различни софтуерни продукти.

ОПИСАНИЕ НА ДИСЦИПЛИНАТА: Учебният материал включва приложните аспекти на криптографските методи и алгоритми, подходи за тяхната имплементация и вграждане в софтуерни продукти. Основни теми: Библиотеки реализиращи криптографски алгоритми; Услуги за сигурност в .NET; Криптографията във софтуерните системи - сертификати, КЕП, сигурни протоколи, автентификация и други. Оценка на сигурността на криптографските алгоритми (КА); Сравнение и избор на КА за конкретни сфери на приложение; Криптоанализ, валидация на криптографски системи;

ПРЕДПОСТАВКИ: Дисциплината се основава на познания на студентите за основните действия на компютърната система и програмиране. Изучени предмети: „Математика“, „Програмни езици” и „Криптографски методи за защита на информацията“.

МЕТОД ЗА ПРЕПОДАВАНЕ: Лекции, изнасяни с помощта на нагледни материали, слайдове в електронен формат, демонстрации и практически примери. Сем. упр. се провеждат като дискусии върху актуални криптографски проблеми с активното участие на всички студенти. Лаб. упражнения, изпълнявани в компютърен учебен клас в екипи, решавайки практически задачи.

МЕТОДИ НА ИЗПИТВАНЕ И ОЦЕНЯВАНЕ: Текущо оценяване на лекции - колоквиум с теоретични въпроси (40%) и на лабораторни упражнения - разработка на проект (60%).

ЕЗИК НА ПРЕПОДАВАНЕ: български

ПРЕПОРЪЧИТЕЛНА ЛИТЕРАТУРА: 1. Лекционни материали, http://cs.tu-sofia.bg/; 2. Jonathan Katz, Yehuda Lindell, *Introduction to Modern Cryptography*, Chapman & Hall/CRC Cryptography and Network Security, CRC Press/Taylor & Francis Group, 2021; 3. Marius Iulian Mihailescu, Stefania Loredana Nita, *Pro Cryptography and Cryptanalysis: Creating Advanced Algorithms with C# and .NET*, Apress, 2021; 4. David Wong, *Real World Cryptography*, (Early Access), 2021.

ХАРАКТЕРИСТИКА НА УЧЕБНАТА ДИСЦИПЛИНА

Наименование на учебната дисциплина: **Сигурност в EDGE базирани IoT мрежи**	Код: **BCS26.2**	Семестър: **8**
Вид на обучението: Лекции (Л), Семинарни упражнения (СУ) Лабораторни упражнения (ЛУ) Курсова работа (КР) – по избор	Семестриален хорариум: Л – 20 часа, СУ – 10 часа, ЛУ – 10 часа	Брой кредити: **4**

ЛЕКТОРИ:
доц. д-р инж. Георги Балабанов (ФТК), тел.: 965 34 56, email: grb@tu-sofia.bg
доц. д-р инж. Камелия Николова (ФТК), тел.: 965 21 34, email: ksi@tu-sofia.bg
Технически университет-София

СТАТУТ НА ДИСЦИПЛИНАТА В УЧЕБНИЯ ПЛАН: Свободно избираема учебна дисциплина от учебния план за обучение на студенти за ОКС „бакалавър“, специалност “Киберсигурност”, професионално направление 5.3 Комуникационна и компютърна техника, област 5. Технически науки.

ЦЕЛИ НА УЧЕБНАТА ДИСЦИПЛИНА: Целта на обучението е да се дадат на студентите в систематизиран вид задълбочени познания по сигурност за IoT мрежи, базирани на EDGE Computing. Студентите, приключили обучението си, трябва да познават мрежовата архитектурата, политиките, стандартите и протоколите свързани със сигурността в IoT мрежите, както и методите за атаки и мерките за тяхното предотвратяване.

ОПИСАНИЕ НА ДИСЦИПЛИНАТА: Основни теми: IoT и Edge архитектура, WPAN не базиран на IP, IP-базирани WPAN и WLAN, Системи и протоколи за комуникация на дълги разстояния (WAN), Предназначение и дефиниция на EDGE, EDGE рутиране и мрежова свързаност, Облачни протоколи за EDGE, Топологии на облаци и мъгла, IoT и EDGE сигурност, Поверителност в Fog/Edge Computing

ПРЕДПОСТАВКИ: Въведение в информационната сигурност, Мрежова сигурност, Сигурност е безжични мрежи

МЕТОД ЗА ПРЕПОДАВАНЕ: Лекции с използване на слайдове, семинарни упражнения, лабораторните упражнения с протоколи.

МЕТОДИ НА ИЗПИТВАНЕ И ОЦЕНЯВАНЕ: Две писмени текущи контролни работи в средата и края на семестъра (общо 70%), Семинарни упражнения (10%), Лабораторни упражнения (20%)

ЕЗИК НА ПРЕПОДАВАНЕ: Български

ПРЕПОРЪЧИТЕЛНА ЛИТЕРАТУРА:

1. P. Lea, *IoT and Edge Computing for Architects (Implementing edge and IoT systems from sensors to clouds with communication systems, analytics, and security)*, 2nd Ed., Packt Publishing, 2020.
2. W. Chang, J. Wu (Editors), *Fog/Edge Computing For Security, Privacy, and Applications*, Advances in Information Security, Springer, 2021.
3. M. Ahmed and P. Haskell-Dowland (Editors), *Secure Edge Computing Applications, Techniques and Challenges*, CRC Press, 2022.

ХАРАКТЕРИСТИКА НА УЧЕБНАТА ДИСЦИПЛИНА

Наименование на учебната дисциплина: **Дигитален маркетинг**	Код: **BCS26.3**	Семестър: **8**
Вид на обучението: Лекции (Л) Семинарни упражнения (СУ) Лабораторни упражнения (СУ) Курсова работа (КР) – по избор	Семестриален хорариум: Л – 20 часа СУ – 10 часа ЛУ – 10 часа	Брой кредити: **4**

ЛЕКТОР(И):

Доц. д-р Михаил Драганов (СФ), тел.: 965 3519, e-mail: mdraganov@tu-sofia.bg

Технически университет-София

СТАТУТ НА ДИСЦИПЛИНАТА В УЧЕБНИЯ ПЛАН: Свободно избираема учебна дисциплина от учебния план за обучение на студенти за ОКС „бакалавър“, специалност “Киберсигурност”, професионално направление 5.3 Комуникационна и компютърна техника, област 5. Технически науки.

ЦЕЛИ НА УЧЕБНАТА ДИСЦИПЛИНА: След завършване на курса студентите трябва да могат да: познават понятийния апарат на дигиталния маркетинг; да могат да анализират пазарните ситуации в Интернет; и съответно да могат да разработват дигитални продуктова, ценова, пласментна и комуникационна политики на дадена бизнес организация.

ОПИСАНИЕ НА ДИСЦИПЛИНАТА: Основни теми: Въведение в дигиталния маркетинг. Дигитален маркетингов процес. Интернет базирани маркетингови проучвания. Маркетингова информационна система. Стратегически маркетинг и планиране в Интернет. Дигитални пазари и пазарна политика. Продуктова политика. Ценова политика. Пласментна политика. Комуникационна политика и социално медиен маркетинг. Поведение на потребителите в Интернет..

ПРЕДПОСТАВКИ: Теория на управлението, Висша математика, Икономика, Информатика, Статистика, Менджмънт, Индустриални производствени системи.

МЕТОД ЗА ПРЕПОДАВАНЕ: Лекции с използване на слайдове и демо-програми, семинарните упражнения с протоколи.

МЕТОДИ НА ИЗПИТВАНЕ И ОЦЕНЯВАНЕ: Оценката се формира както следва: 80 % от показаните знания по време на изпита и 20 % от работата по време на семинарните упражнения. По време на семинарните упражнения се провеждат два контролни теста.

ЕЗИК НА ПРЕПОДАВАНЕ: български

ПРЕПОРЪЧИТЕЛНА ЛИТЕРАТУРА: 1. Котлър. Ф., Картаджая. Х., Сетиаван. А. Маркетинг 3.0, Locus, София, 2010г. ISBN 46127778; 2. Котлър. Ф., Картаджая. Х., Сетиаван. А. Маркетинг 4.0, Locus, София, 2019г. ISBN 9789547832893; 3 Kotler,Ph. Kartajaya, H., Setiawan, I. Marketing 5.0: Technology for Humanity, 2021, ISBN-10: 1119668514