ХАРАКТЕРИСТИКА НА УЧЕБНАТА ДИСЦИПЛИНА

Наименование на учебната дисциплина: **Въведение в програмирането**	Код: **MCSPC21**	Семестър: **1**
Вид на обучението: Лекции (Л) Лабораторни упражнения (ЛУ)	Семестриален хорариум: Л – 15 часа ЛУ – 8 часа	Брой кредити: **5**

ЛЕКТОР(И):
Доц. д-р инж. Явор Томов (ФКСТ)), тел.: 965 2606, e-mail: : yavor_tomov@tu-sofia.bg
Технически университет-София

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

ЦЕЛИ НА УЧЕБНАТА ДИСЦИПЛИНА: Целта на учебната дисциплина е студентите да изучат фундаментални понятия за използване на компютрите и придобиване на навици за съвременни технологии на програмиране. Те ще могат да прилагат подходите, методите и техническите средства и основните принципи на структурния подход в програмирането и реализацията им със средствата на конкретен алгоритмичен език от високо ниво. В края на обучението си студентът ще: притежава умения за използване на алгоритмичен език от високо ниво; познава основите на структурния подход в програмирането; познава и използва основните библиотеки на език от високо ниво за програмиране; може да разработва програми като прилага обектно-ориентирания подход; има познания за технологията за прихващане и обработка на изключения и грешки в програмата си; познава принципите на работа за съхранение и обработка на данни; решава типични инженерни задачи със средствата на език за програмиране от високо ниво.

ОПИСАНИЕ НА ДИСЦИПЛИНАТА: Въведение в програмирането е задължителен фундаментален учебен курс от магистърската учебна програма на направление 5.3 „Комуникационна и компютърна техника“. Знанията и уменията по Въведение в програмирането създават предпоставки за програмно решаване на практически задачи и многостранна реализация на студентите в областта на информационните технологии.

ПРЕДПОСТАВКИ: Знания по математика и информационни технологии.

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

МЕТОДИ НА ИЗПИТВАНЕ И ОЦЕНЯВАНЕ: Текуща оценка.

ЕЗИК НА ПРЕПОДАВАНЕ: български

ПРЕПОРЪЧИТЕЛНА ЛИТЕРАТУРА:
1. Michael & Eric Scratch, PYTHON ALGORITHMS: A Complete Guide to Learn Python for Data Analysis, Machine Learning, and Coding from Scratch (Python programming language), Independently published, 1st Ed., 2020. 2. Michael & Eric Scratch, PYTHON PROGRAMMING FOR BEGINNERS: Your Personal Guide for Getting into Programming, Level Up Your Coding Skills from Scratch and Use Python Like A Mother Language (Python programming language), Independently published, 1st Ed., 2020. 3. Michael & Eric Scratch, Coding Python: The Ultimate Tool To Progress Your Python Programming From Good To Great While Making Coding In Scratch Look Easy (Python programming language), Independently published, 1st Ed., 2020.

ХАРАКТЕРИСТИКА НА УЧЕБНАТА ДИСЦИПЛИНА

Наименование на учебната дисциплина: **Синтез и анализ на алгоритми**	Код: **MCSPC22**	Семестър: **1**
Вид на обучението: Лекции (Л) Лабораторни упражнения(ЛУ)	Семестриален хорариум: Л – 15 часа ЛУ – 8 часа	Брой кредити: **5**

ЛЕКТОР(И):

Проф. д-р инж. Огнян Наков (ФКСТ), тел.: 965 3613, e-mail: nakov@tu-sofia.bg;
Доц. д-р инж. Георги Запрянов, тел. 965 2680, e-mail: gszap@tu-sofia.bg;
Доц. д-р инж. Иван Станков (ФКСТ), тел.: 965 2682, e-mail: istankov@tu-sofia.bg
Технически университет-София

СТАТУТ НА ДИСЦИПЛИНАТА В УЧЕБНИЯ ПЛАН: Задължителна учебна дисциплина от учебните планове за редовни студенти и за ОКС „магистър“, специалност “Киберсигурност и превенция на киберпрестъпления” на Факултет по компютърни системи и технологии (ФКСТ) на Технически Университет – София, професионално направление 5.3 Комуникационна и компютърна техника, област 5. Технически науки.

ЦЕЛИ НА УЧЕБНАТА ДИСЦИПЛИНА: Придобиване на умения за алгоритмизиране на проблем, анализ и оценка на алгоритми и синтез на програми, базирани на такива алгоритми. Студентите се запознават с основни групи алгоритми: обработка на числа, сортировки, търсене, хеширане, дървовидни структури, рекурсии, списъчни структури, граф и обработка на графи. Проиграват се и анализират класически алгоритмични решения. Оценяват се различни решения на един проблем.

ОПИСАНИЕ НА ДИСЦИПЛИНАТА: Курсът запознава студентите с теорията на алгоритмизиране, анализ на сложността и ресурсоемкостта на алгоритми и синтез на оптимални алгоритми. Разглеждат се класически групи от алгоритми: обработка на числа, сортировки, търсене, хеширане, дървовидни структури, рекурсии, списъчни структури,граф и обработка на графи. Проиграват се и анализират класически алгоритмични решения.

ПРЕДПОСТАВКИ: Изискват се начални познания по програмиране на C и C++.

МЕТОД ЗА ПРЕПОДАВАНЕ: Лекции в мултимедиен вариант (медиен проектор), разработен и достъпен уеб сайт с лекционното и практическо съдържание на дисциплината.

МЕТОДИ НА ИЗПИТВАНЕ И ОЦЕНЯВАНЕ: Писмен изпит със задача.

ЕЗИК НА ПРЕПОДАВАНЕ: Български

ПРЕПОРЪЧИТЕЛНА ЛИТЕРАТУРА:

1.Clifford A. Shaffer, Data Structures and Algorithm Analysis, 2013; 2.Sandeep Sen, Lecture Notes for Algorithm Analysis and Design, 2013; 3.Sara Baase, Computer Algorithms: Introduction to Design and Analysis, 2009; 4.Samir Khuler, Design and Analysis of Algorithms, 2012; 5.A.A.Puntambekar, Design and Analysis of Algorithms, 2010; 6.Стойчев Ст., Синтез и анализ на алгоритми и програми, издателство на ТУ- София; 7. Sedgewick R., Wayne K., Algorithms,Addison-Wesley Professional 2011; 8.Dasgupta, S., C.H. Papadimitriou, and U.V. Vazirani. Algorithms, 2006; 9.Thomas Runkler, Data Analytics, 2012.

ХАРАКТЕРИСТИКА НА УЧЕБНАТА ДИСЦИПЛИНА

Наименование на учебната дисциплина: **Анализ и управление на риска**	Код: **MCSPC23**	Семестър: **1**
Вид на обучението: Лекции (Л) Лабораторни упражнения (ЛУ)	Семестриален хорариум: Л –15 часа ЛУ – 8 часа	Брой кредити: **5**

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: Задължителна учебна дисциплинаот учебния план/учебните планове за обучение на студенти за ОКС „магистър“, специалност “Киберсигурност и превенция на киберпрестъпления”, 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: **Програмни технологии за сигурен код**	Код: **MCSPC24**	Семестър: 1
Вид на обучението: Лекции (Л) Лабораторни (ЛУ)	Семестриален хорариум: Л – 15 часа ЛУ – 8 часа	Брой кредити: **5**

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: задължителна учебна дисциплина от учебния план за обучение на студенти за ОКС „магистър“, специалност “Киберсигурност и превенция на киберпрестъпления”, 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: **Интернет и социални мрежи**	Код: **MCSPC25**	Семестър: **1**
Вид на обучението: Лекции (Л) Лабораторни упражнения (ЛУ)	Часове за семестър: Л – 15 часа, ЛУ – 8 часа	Брой кредити: **5**

ЛЕКТОРИ:

проф. д-р Георги Илиев (ФТК), тел. 965 3029, email: gli@tu-sofia.bg

гл. ас. д-р Димитрия Михайлова (ФТК), тел. 965 3029, email: dam@tu-sofia.bg

Технически Университет-София

СТАТУТ НА ДИСЦИПЛИНАТА В УЧЕБНИЯ ПЛАН: Задължителна дисциплина за редовни студенти по специалност "Киберсигурност и превенция на киберпрестъпления" за образователно-квалификационната степен "магистър".

ЦЕЛИ НА УЧЕБНАТА ДИСЦИПЛИНА:

Целта на обучението по "Интернет и социални мрежи" е студентите да изучат основни принципи на изграждане, развитие и класификация на мрежовите технологии; еталонни модели за свързване на отворени системи; комуникационни протоколи в мрежовите технологии.

ОПИСАНИЕ НА ДИСЦИПЛИНАТА:

По време на курса се изучават въведение в мрежовите технологии. Принципи на изграждане, състояние, развитие, класификация, стандарти и организации за стандартизация. Основни топологии, сравнителен анализ. Еталонни модели за свързване на отворени системи. Принципи на изграждане. Предназначение и функции на отделните нива. Мрежа Ethernet. Основни принципи на изграждане и функциониране. Стандарти, тенденции и развитие. Приложение на Ethernet технологията в различни мрежи. Основни характеристики на Интернет технологията. Използвани протоколи – роля и функциониране. Адресиране в IP мрежи. Разпределение и преизползване на адресното пространство. Интернет като комуникационна среда. Работа във Фейсбук, Туитър и други социални мрежи. Въведение в анализа на социалните мрежи. Социални мрежи за бизнес и професионална употреба.

ПРЕДПОСТАВКИ: Необходими са основни познания по математика, компютърни системи, сигнали и системи.

МЕТОД ЗА ПРЕПОДАВАНЕ: Лекции с използване на слайдове (предварително предоставени на студентите), подпомогнати от електронни материали. Самостоятелна подготовка и възлагане на работа по актуални проблеми (екипно ориентиран подход). Лабораторни упражнения с протоколи.

МЕТОДИ НА ИЗПИТВАНЕ И ОЦЕНЯВАНЕ: Обучението се контролира чрез оценка, която се формира от две съставки: резултат от текущ контрол с коефициент на тежест 0,7 и оценка от лабораторните упражнения с коефициент на тежест 0,3.

ЕЗИК НА ПРЕПОДАВАНЕ: български

ПРЕПОРЪЧИТЕЛНА ЛИТЕРАТУРА:

1. Dodd A., Essential Guide to Telecommunications – The, 6th Edition, Pearson, 2019, ISBN 978-0-13-450778-1. **2.** Ibe O., Fundamentals of Data Communication Networks, Wiley, 2018, ISBN 978-1-1194-3625-6. **3.** Valdar A., Understanding Telecommunications Networks – 2nd Edition, The Institution of Engineering and Technology, 2017, ISBN 978-1-78561-165-0. **4.** Sibley M., Modern Telecommunications: Basic Principles and Practices, CRC Press, 2018, ISBN 978-1-1385-7882-1. **5.** Goralski W., The Illustrated Network: How TCP/IP Works in a Modern Network, Morgan Kaufman, 2017, ISBN 978-0-12-811027-0.

ХАРАКТЕРИСТИКА НА УЧЕБНАТА ДИСЦИПЛИНА

Наименование на дисциплината: **Електронни системи за сигурност**	Код: **MCSPC26**	Семестър: **1**
Вид на обучението: Лекции (Л) Лабораторни упражнения (ЛУ)	Часове за семестър: Л - 15 часа ЛУ - 8 часа	Брой кредити: **5**

ЛЕКТОР:

Проф. д-р инж. Георги Илинчев Попов (ФКСТ), тел: 029653525, popovg@tu-sofia.bg,
Технически университет - София

СТАТУТ НА ДИСЦИПЛИНАТА В УЧЕБНАТА ПРОГРАМА: Задължителна дисциплина за редовни и задочни студенти от специалност "Киберсигурност и превенция на киберпрестъпления" на Факултет по Компютърни системи и технологии на ТУ-София за образователно-квалификационната степен "магистър".

ЦЕЛИ НА УЧЕБНАТА ПРОГРАМА: Целта на обучението е студентите да се запознаят със съвременните електронни системи за сигурност, тяхната структура и функциониране, сфери на приложение и нормативни актове, свързани с тях.

ОПИСАНИЕ НА ДИСЦИПЛИНАТА: В курса се изучават фундаменталните понятия, отнасящи се до системите за сигурност: системи срещу проникване и взлом в т.ч. контролни панели и детектори, пожароизвестителни и пожарогасителни системи, системи за контрол на достъпа, системи за видеоконтрол и видеодетекция, периметрови системи, индустриални алармени системи и др. Дискутираните концепции се илюстрират с примери от реални системи – Paradox, DSC, Aritech, Sony, JVC, HikVision и др.

ПРЕДПОСТАВКИ: При изучаването на дисциплината се предполага, че студентите са придобили основни познания по физика.

МЕТОД НА ПРЕПОДАВАНЕ: Изнасят се лекции, онагледявани с нагледни материали и видеопроектор. Лабораторните упражнения се провеждат в компютърни зали, съгласно ръководството, и проверка на резултатите от преподавателя. По проектите студентите получават консултации.

МЕТОДИ ЗА ИЗПИТВАНЕ И ОЦЕНЯВАНЕ: изпит

ЕЗИК ЗА ПРЕПОДАВАНЕ: Български, Английски

ПРЕПОРЪЧИТЕЛНА ЛИТЕРАТУРА: http://sopko.tu-sofia.bg >> Дисциплини >>
Охранителни системи; 2. Thomas L. Norman, Integrated Security Systems Design: Concepts, Specifications, and Implementation, Butterworth-Heinemann –London UK, 2011 г.; 3. Corky Binggeli, Building Systems for Interior Designers, John Wiley & Sons, 11.10.2011; 4. Попов Г., Трифонов Р., Електронни системи за сигурност, Издателство на ТУ-София, 2010; 5. Петков Б., Алармени системи I и II част , София, 1998; 6. Попов Г., Алармени системи, София, издателство на ТУ-София, 2007; 7. Capel V., Security Systems and Intruder Alarms, Oxford, 1992.,

ХАРАКТЕРИСТИКА НА УЧЕБНАТА ДИСЦИПЛИНА

Наименование на учебната дисциплина: **Блокчейн технологии**	Код: **MCSPC27**	Семестър: **2**
Вид на обучението: Лекции (Л) Лабораторни упражнения (ЛУ)	Семестриален хорариум: Л – 15 часа ЛУ – 8 часа	Брой кредити: **5**

ЛЕКТОР(И):
Доц. д-р инж. Явор Томов (ФКСТ), тел.: 965 2606, email: yavor_tomov@tu-sofia.bg
Технически университет-София

СТАТУТ НА ДИСЦИПЛИНАТА В УЧЕБНИЯ ПЛАН: Задължителна дисциплина от учебния план за обучение на студенти по специалност "Киберсигурност и превенция на киберпрестъпления", на Факултет по Компютърни системи и технологии на Технически Университет – София за образователно-квалификационна степен "магистър".

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 изпит.

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: **Биометрични системи**	Код: **MCSPC28**	Семестър: **2**
Вид на обучението: Лекции (Л) Лабораторни упражнения (ЛУ)	Семестриален хорариум: Л – 15 часа ЛУ – 8 часа	Брой кредити: **5**

ЛЕКТОРИ:
Проф. д-р инж. Снежана Плешкова (ФТК), тел.: 965 2274, e-mail: snegpl@tu-sofia.bg
доц. д-р Агата Манолова, ФТК, тел:02 9652274, е-мейл: amanolova@tu-sofia.bg
гл. ас. д-р Никол Христова, ФТК, тел:02 9652274, е-мейл: nicole.christoff@tu-sofia.bg
гл. ас. д-р Николай Нешов, ФТК, тел:02 9652274, е-мейл: nneshov@tu-sofia.bg
Технически университет-София

СТАТУТ НА ДИСЦИПЛИНАТА В УЧЕБНИЯ ПЛАН: Биометрични системи е задължителна учебна дисциплина от учебния план за обучение на студентите за ОКС „магистър“, специалност „Киберсигурност и Превенция на киберпрестъпления”, професионално направление 5.3 Комуникационна и компютърна техника, област 5. Технически науки.

ЦЕЛИ НА УЧЕБНАТА ДИСЦИПЛИНА: Целта на дисциплината е да запознае студентите със системите, използващи биометрична информация, видовете биометрични данни, тяхната обработка и разпознаване, проектиране на биометричини бази данни, моделиране и визуализация на биометрича информация. Студентът ще придобие способността да разбира структурата и функционалността на биометричните системи, най-добрите практики относно внедряването в решения с общо предназначение и със специфична нужди към конкретните случаи на употреба.

ОПИСАНИЕ НА ДИСЦИПЛИНАТА: Основни теми: Общ преглед на биометричните системи -Дизайн на биометрични системи -Удостоверяване и идентификация -Анализ на производителността -Биометрични характеристики: пръстов отпечатък, вена, лице 2D/3D, ирис, ретина -Поведенчески характеристики: Динамика на натискане на клавиш, походка, подпис, глас -Мултимодална биометрия -Непрекъснато биометрично удостоверяване -Качество на биометричните проби -Поверителност и защита -Атаки: артефакти и възможности за имитация -Биометрични стандарти -Биометрични приложения.

ПРЕДПОСТАВКИ: Въведение в програмирането, Системи за сигурност, Изкуствен интелект и киберсигурност.

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

МЕТОДИ НА ИЗПИТВАНЕ И ОЦЕНЯВАНЕ: Обучението по учебната дисциплина се контролира чрез **оценка**, която се формира от три съставки: две контролни работи с коефициент на тежест 0,4 и работа по време на лабораторните упражнения с коефициент на тежест 0,2.

ЕЗИК НА ПРЕПОДАВАНЕ: български/английски

ПРЕПОРЪЧИТЕЛНА ЛИТЕРАТУРА:
1. R. Jiang, S. Al-maadeed, A. Bouridane, D. Crookes, A. Beghdadi, *Biometric Security and Privacy: Opportunities & Challenges in The Big Data Era*, Springer, 2016 ; ISBN 9783319473017; 2. D. Zhang, G. Lu, L. Zhang, *Advanced Biometrics*, Springer, 2017, ISBN 9783319615455; 3. B. Bhanu, A. Kumar, *Deep Learning for Biometrics*, 2017, Springer, ISBN 9783319616575; 4. G.R. Sinha, *Advances in Biometrics: Modern Methods and Implementation Strategies*, 2019, Springer Nature, ISBN 9783030304362; 5. T. Bourlai, P. Karampelas, V. Patel: Securing Social Identity in Mobile Platforms: Technologies for Security, Privacy and Identity Management, Springer, 2020, ISBN 9783030394899.

ХАРАКТЕРИСТИКА НА УЧЕБНАТА ДИСЦИПЛИНА

Наименование на учебната дисциплина: **Приложна криптография**	Код: **MCSPC29**	Семестър: **2**
Вид на обучението: Лекции (Л) Лабораторни упражнения (ЛУ)	Семестриален хорариум: Л – 15 часа ЛУ – 8 часа	Брой кредити: **5**

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: Приложна криптография е задължителна учебна дисциплина от учебния план за обучение на студентите за ОКС „магистър“, специалност „Киберсигурност и Превенция на киберпрестъпления”, 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 във 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: изпит.

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: **Мрежова и информационна сигурност**	Код: **MCSPC30**	Семестър: **2**
Вид на обучението: Лекции (Л) Лабораторни упражнения (ЛУ)	Семестриален хорариум: Л – 15 часа ЛУ – 8 часа	Брой кредити: **5**

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 учебна дисциплина от учебния план за обучение на студенти за ОКС „магистър“, специалност “Киберсигурност и превенция на киберпрестъпления”, професионално направление 5.3Комуникационна и компютърна техника, област, област 5. Технически науки.

ЦЕЛИ НА УЧЕБНАТА ДИСЦИПЛИНА: Дисциплината “Мрежова и информационна сигурност” има за цел запознаване на студентите с основните понятия, стандарти и техники в областта на мрежовата и информационна сигурност. Студентите ще се запознаят с нормативна база, която регулира дейността на българските структури на сигурност. Целта на курса е да създадат у студентите знания и умения, свързани с добрите практики при прилагането на съвременни компютърни и информационни технологии в системите за сигурността.

ОПИСАНИЕ НА ДИСЦИПЛИНАТА: Курсът „Основи на киберсигурността“ представя основните направления на сигурността 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 сигурност за автоматизираните информационни системи, стандарти и заплахи срещу мрежовата и информационна сигурност. Предвидените лабораторни 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 и демо-програми, лабораторните упражнения с помощта на компютър.

МЕТОДИ НА ИЗПИТВАНЕ И ОЦЕНЯВАНЕ: текуща оценка.

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, Г. Цочев, Методи на изкуствения интелект за мрежова и информационна сигурност, Монография, изд. Авангард Прима, 2018, 168 стр., ISBN: 978-619-160-936-9; 3. **Румен Трифонов** и др., Мрежова и Информационна Сигурност, Авангард прима, 2013; 4. http://www.enisa.europa.eu/.; 5. ISO/IEC 27032:2012, Information technology — Security techniques — Guidelines for cybersecurity; 6. https://www.paloaltonetworks.com/cyberpedia/what-is-cyber-security.

ХАРАКТЕРИСТИКА НА УЧЕБНАТА ДИСЦИПЛИНА

Наименование на учебната дисциплина: **Анализ и оценка на уязвимости в киберпространството**	Код: **MCSPC31**	Семестър: 2
Вид на обучението: Лекции (Л) Лабораторни (ЛУ)	Семестриален хорариум: Л –15 часа ЛУ – 8 часа	Брой кредити: **5**

ЛЕКТОР(И):

Доц. д-р инж. Иван Станков (ФКСТ), тел.: 965 XXXX, e-mail: istankov@tu-sofia.bg

Доц. д-р инж. Върбинка Стефанова- Стоянова (ФКСТ), тел.: 965 XXXX, e-mail: vvstoyanova@tu-sofia.bg

Технически университет-София

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

ЦЕЛИ НА УЧЕБНАТА ДИСЦИПЛИНА: Цел на дисциплината „Анализ и оценка на уязвимости в киберпространството“ е да предостави на студентите практическо и научно-изследователско ноу-хау в сферата на анализа, оценката и управлението на уязвимости в работните и съпътстващите процеси, с акцент върху значението и динамизма на бъдещата работна среда, както и разбиране за концепциите и техниките, включени в анализа иоценката на уязвимостите в контекста на киберсигурността.

ОПИСАНИЕ НА ДИСЦИПЛИНАТА: Основни теми: Въведение: оценката на уязвимостта, основен компонент на всяка стратегия за киберсигурност Основно разграничение между уязвимости и заплахи. Видове уязвимости, включително софтуерни и хардуерни уязвимости, водещи до различни видове заплахи. Тестове за проникване и сканиране на уязвимости. Проактивно идентифициране и адресиране на уязвимости. Приоритизиране на уязвимостите. Категоризиране на уязвимости в компютърни системи, мрежи и приложения. Фази в процеса на оценка и управление на уязвимостта..

ПРЕДПОСТАВКИ: Информационни системи, бизнес 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: Постигането на поставената цел на обучението по учебната дисциплина се контролира чрез изпит (общо 90%) и лабораторни упражнения (10%).

ЕЗИК НА ПРЕПОДАВАНЕ: български

ПРЕПОРЪЧИТЕЛНА ЛИТЕРАТУРА: Network Security Discovering the Optimal & Secure Path by Vulnerability Analysis in Dynamic Network Through Attack Graphs, Gouri R. Patil, |Jul 18, 2022, Vulnerability Analysis A Complete Guide, 2020 Edition, Gerardus Blokdyk, Apr 21, 2021, Vulnerability Analysis and Risk Assessment: For Dynamic Nonmotorized Human Travel Activity Networks, Trends in Social Network Analysis, Information Propagation, User Behavior Modeling, Forecasting, and Vulnerability, Assessment, Rokia Missaoui, Talel Abdessalem, Matthieu Latapy, |2017.

ХАРАКТЕРИСТИКА НА УЧЕБНАТА ДИСЦИПЛИНА

Наименование на учебната дисциплина: **Изкуствен интелект и киберсигурност**	Код: **MCSPC32**	Семестър: **2**
Вид на обучението: Лекции (Л) Лабораторни упражнения (ЛУ)	Семестриален хорариум: Л – 15 часа ЛУ – 8 часа	Брой кредити: **5**

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 учебна дисциплина от учебния план за обучение на студенти за ОКС „магистър“, специалност “Киберсигурност и превенция на киберпрестъпления”, 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: текуща оценка.

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.