

## ХАРАКТЕРИСТИКА НА УЧЕБНАТА ДИСЦИПЛИНА

Наименование на учебната дисциплина: <b>Принципи на предаването на информация</b>	Код: <b>BCS01</b>	Семестър: <b>5</b>
Вид на обучението: Лекции (Л) Лабораторни упражнения (ЛУ) Курсова работа (КР) - по избор	Семестриален хорариум: Л – 30 часа ЛУ – 15 часа	Брой кредити: <b>5</b>
Курсов проект (КП) – по избор	Код: <b>BCS07</b>	Брой кредити: <b>2</b>

### ЛЕКТОР(И):

Доц. д-р инж. Павлина Колева (ФТК), тел.: 965 2134, e-mail: [p\\_koleva@tu-sofia.bg](mailto:p_koleva@tu-sofia.bg)

Доц. д-р инж. Росен Милетиев (ФТК), тел.: 965 2146, e-mail: [miletiev@tu-sofia.bg](mailto: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:** След завършване на курса студентите ще познават основните принципи от теорията на предаване на информацията по комуникационни канали, ще могат да определят основните понятия, величини, показатели и зависимости от теорията на предаване на информацията, ще познават теорията за оптимално кодиране, принципите на шумоустойчивото кодиране, принципите на методите и средствата за защита (криптиране) на съобщенията, на комуникациите с разширен спектър на сигналите, на спектрално ефективните методи за модулация и кодиране.

**ОПИСАНИЕ НА ДИСЦИПЛИНАТА:** Основни теми: Въведение в теорията на предаване на информацията; Информационна оценка на комуникационни канали; Източници на съобщения; Кодиране на източника, оптимално кодиране; Комуникационни канали, видове, математически модели, пропускателна способност; Особенности на предаване на аналогови и цифрови сигнали по комуникационни канали; Специфичните за телекомуникациите аналогови и дискретни модуляции; Шумоустойчиво кодиране; Принципи на защита (криптиране) на съобщенията; Предаване на сигнали с разширен спектър; Спектрално ефективни методи за модулация и кодиране.

**ПРЕДПОСТАВКИ:** Математика, Теория на вероятностите, Булева алгебра, Физика, Електротехника, Сигнали и системи.

**МЕТОД ЗА ПРЕПОДАВАНЕ:** Лекции по класическия начин и с помощта на мултимедия, лабораторни упражнения, по време на които студентите решават проблеми, свързани с преподадения лекционен материал.

**МЕТОДИ НА ИЗПИТВАНЕ И ОЦЕНЯВАНЕ:** Изпит след края на семестъра (80%), Работа по време на семестъра, включваща лабораторни упражнения и курсова работа по избор (20%), Курсов проект по избор с отделна оценка.

**ЕЗИК НА ПРЕПОДАВАНЕ:** Български

**ПРЕПОРЪЧИТЕЛНА ЛИТЕРАТУРА:** 1. Пулков В., Колева П. Основи на предаване на информацията. Нови Знания. 2014. ISBN: 9789549315974; 2. Sklar B., Harris F. Digital Communications: Fundamentals and Applications (Communications Engineering & Emerging Technology Series from Ted Rappaport), 3rd edition. Pearson. 2020. ISBN: 978-0134588568; 3. Proakis J. G., Salehi M. Fundamentals of Communication Systems, Global Edition, 2nd edition. Pearson. 2014. ISBN: 978-1292015682; 4. Gray R. M. Entropy and Information Theory, 2nd edition, Springer. 2011. ISBN: 978-1441979698.

## ХАРАКТЕРИСТИКА НА УЧЕБНАТА ДИСЦИПЛИНА

Наименование на учебната дисциплина: <b>Мрежова сигурност</b>	Код: <b>BCS02</b>	Семестър: <b>5</b>
Вид на обучението: Лекции (Л), Лабораторни упражнения (ЛУ), Курсова работа (КР) – по избор	Семестриален хорариум: Л – 30 часа, ЛУ – 30 часа	Брой кредити: <b>5</b>
Курсов проект (КП) – по избор	Код: <b>BCS07</b>	Брой кредити: <b>2</b>

### ЛЕКТОРИ:

доц. д-р инж. Георги Балабанов (ФТК), тел.: 965 34 56, email: [grb@tu-sofia.bg](mailto:grb@tu-sofia.bg)  
доц. д-р инж. Златка Вълкова-Джарвис (ФТК), тел.: 965 26 62, email: [zvz@tu-sofia.bg](mailto:zvz@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 по мрежова сигурност. Студентите, приключили обучението си, трябва да познават мрежовата архитектурата, политиките, стандартите и протоколите свързани с мрежовата сигурност, методите за атаки и мерките за тяхното предотвратяване.

**ОПИСАНИЕ НА ДИСЦИПЛИНАТА:** Основни теми: Въведение в мрежовата сигурност, Сигурност и защита на слой 2, Сигурност и защита на слой 3 и слой 4, Криптография, Удостоверяване, Политики за сигурност в комуникационните мрежи, Частни виртуални мрежи, Сигурност на маршрутизацията (BGP). Мониторинг и защитни стени, Системи за детектиране на интрузия, Управление на мрежовата сигурност, Защита на уеб браузъра и уеб сървър, Поверителност, Червеи, вируси, ботнети, Защита на Имейл/ IM/ Онлайн социални мрежи / Криптовалути

**ПРЕДПОСТАВКИ:** Основи на мрежовите технологии, Компютърни системи.

**МЕТОД ЗА ПРЕПОДАВАНЕ:** Лекции с използване на слайдове, лабораторните упражнения с протоколи и курсов проект / 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. Aditya Mukherjee. *Network Security Strategies*, Packt Publishing, 2020. 2 William Stallings, *Cryptography and Network Security: Principles and Practice*, Pearson, 2017 3. Brotherston L., A. Berlin., *Defensive Security Handbook: Best Practices for Securing Infrastructure*. O'Reilly Media. 2017. 4. Bianco, David J.; Sanders, Chris; Smith, Jason. *Applied network security monitoring collection, detection, and analysis*, Elsevier, 2014. 5. Debashis Ganguly, *Network and application security : fundamentals and practices*, CRC Press, 2012. 6. Мерике Каео, *Проектиране на мрежова сигурност*, СофтПрес, 2006.

## ХАРАКТЕРИСТИКА НА УЧЕБНАТА ДИСЦИПЛИНА

Наименование на учебната дисциплина: <b>Сигурност на физичния слой в безжичните комуникации</b>	Код: <b>BCS03</b>	Семестър: <b>5</b>
Вид на обучението: Лекции (Л) Лабораторни упражнения (ЛУ) Курсова работа (КР) – по избор	Семестриален хорариум: Л – 30 часа ЛУ – 15 часа	Брой кредити: <b>4</b>
Курсов проект (КП) – по избор	Код: <b>BCS07</b>	Брой кредити: <b>2</b>

**ЛЕКТОРИ:** Проф. д-р инж.Илия Илиев (ФТК), тел.: 965 22 76, e-mail: [igiliev@tu-sofia.bg](mailto:igiliev@tu-sofia.bg)  
Доц. д-р инж. Марин Неделчев (ФТК), тел.: 965 26 86, e-mail: [mnedelchev@tu-sofia.bg](mailto:mnedelchev@tu-sofia.bg)  
Гл. ас. д-р инж. Лудвиг Лубих (ФТК), тел.: 965 3153, e-mail: [lvl@tu-sofia.bg](mailto:lvl@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 имат фундаментални знания относно обезпечаване на сигурността във физическия слой на безжичните радиочестотни технологии, алгоритмите и устройства за реализирането на основната им функции: да осъществят сигурна радиовръзка в сложна вариантна и когнитивна радио среда.

**ОПИСАНИЕ НА ДИСЦИПЛИНАТА:** Основни теми: Безжични комуникации (радиокомуникации): радиочестотен спектър и разпределение, разпространение на електромагнитните вълни, федингови канали и тяхното моделиране; Формиране на радиочестотни сигнали: цифрови модуляции и демодуляции, OFDM; методи за преизползване на канала за връзка, TDMA, FDMA, CDMA OFDMA, скрамблиране, кодиране за сигурни канали; Основни алгоритми за сигурни радиокомуникационни предаватели и приемници. В дисциплината се разглеждат генерирането на ключове за безжични канали за връзка, използване на MIMO алгоритми като технология за постигане на сигурност, сигурни системи с разширен спектър, кооперативни сигурни безжични комуникации.

**ПРЕДПОСТАВКИ:** Сигнали и системи, Основи на мрежовите технологии, Измервания в информационните и комуникационните технологии, Мрежова сигурност, Принципи на предаването на информация.

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

**МЕТОДИ НА ИЗПИТВАНЕ И ОЦЕНЯВАНЕ:** Две едночасови писмени текущи оценки в средата и края на семестъра (общо 62%), лабораторни упражнения (18%), курсова работа с две задачи (20%). Защита на курсов проект (100%)

**ЕЗИК НА ПРЕПОДАВАНЕ:** български/английски

**ПРЕПОРЪЧИТЕЛНА ЛИТЕРАТУРА:** 1. X. Zhou, L. Song, and Y. Zhang (Eds.), Physical Layer Security in Wireless Communications, CRC Press, 2018., 2. R. F. Schaefer, H. Boche, A. Khisti, and H. V. Poor (Eds), Information Theoretic Security and Privacy of Information Systems, Cambridge University Press, 2017. 3. T. Q. Duong, X. Zhou, and H. V. Poor (Eds.), Trusted Communications with Physical Layer Security for 5G and Beyond, IET, 2016.

## ХАРАКТЕРИСТИКА НА УЧЕБНАТА ДИСЦИПЛИНА

Наименование на учебната дисциплина: <b>Сигурност на операционни системи</b>	Код: <b>BCSE04</b>	Семестър: <b>5</b>
Вид на обучението: Лекции (Л) Лабораторни (ЛУ) Курсова работа (КР) – по избор	Семестриален хорариум: Л – 30 часа ЛУ – 15 часа	Брой кредити: <b>4</b>
Курсов проект (КП) – по избор	Код: <b>BCSE07</b>	Брой кредити: <b>2</b>

### **ЛЕКТОР(И):**

Доц. д-р инж. Надежда Ангелова (ФКСТ), тел.: 965 2017, e-mail: [n\\_angelova@tu-sofia.bg](mailto:n_angelova@tu-sofia.bg)  
Технически университет-София

**СТАТУТ НА ДИСЦИПЛИНАТА В УЧЕБНИЯ ПЛАН:** Задължителна 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 запознае студентите със структурата на класическа операционна система и основните прилагани подходи за сигурност. Сигурност в облачни структури, виртуализация и контейнеризация

**ОПИСАНИЕ НА ДИСЦИПЛИНАТА:** Основни теми: Сигурност на компютърна и операционната система. Управление на потребители, защитни стени, защитени мрежи, защита на файлови системи. Сигурност в контейнери и технология за контейнеризации на ОС. Сигурност в облачни структури, вградени системи и контролери. Сигурнос в мобилни ОС.

**ПРЕДПОСТАВКИ:** Владее на език за програмиране, както и програмна среда за разработка на софтуерни приложения. Опит с работа с различни видове ОС

**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:** Два текущи писмен изпита по 90 мин. – състоящ се от два теоритични въпроса (60%) и задача (40%) (общо 100%) – първи изпит и два въпроса втори контролен изпит (по 50% на въпрос). Лабораторни упражнения (0%), курсова работа (0%). Оценката се формира само от резултата от двата изпита, курсовата работа е само за заверка на семестъра, както и упражненията, те не влияят на общата оценка.

**ЕЗИК НА ПРЕПОДАВАНЕ:** български/английски

**ПРЕПОРЪЧИТЕЛНА ЛИТЕРАТУРА:** Operating System Concepts by Abraham Silberschatz, Peter B. Galvin and Greg Gagne (Dec 17, 2012), Modern Operating Systems (4th Edition) by Andrew S. Tanenbaum and Herbert Bos (Mar 20, 2014), Linux for Beginners: An Introduction to the Linux Operating System and Command Line by Jason Cannon (Jan 2, 2014)

## ХАРАКТЕРИСТИКА НА УЧЕБНАТА ДИСЦИПЛИНА

Наименование на учебната дисциплина: <b>Обектно-ориентирано програмиране</b>	Код: <b>BCS05</b>	Семестър: <b>5</b>
Вид на обучението: Лекции (Л) Лабораторни упражнения (ЛУ) Курсова работа (КР) – по избор	Семестриален хорариум: Л – 30 часа ЛУ – 30 часа	Брой кредити: <b>5</b>
Курсов проект (КП) – по избор	Код: <b>BCS07</b>	Брой кредити: <b>2</b>

### ЛЕКТОР(И):

Проф. д-р инж. Огнян Наков Наков (ФКСТ), тел.: 965 3613, e-mail: [nakov@tu-sofia.bg](mailto: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 „бакалавър“, специалност “Киберсигурност“ професионално направление 5.3 Комуникационна и компютърна техника, област 5. Технически науки.

**ЦЕЛИ НА УЧЕБНАТА ДИСЦИПЛИНА:** Курсът запознава студентите с теорията и практиката на програмиране в обектна среда. Базира се на езика C++ с последните актуализации на стандарта. Разглеждат се и съпътстващи теми: софтуерни контракти, принципи и практики на обектния софтуерен дизайн, генетични и шаблонизирани типове; Lambda-изрази; разполагане и управление на обекти в паметта, както и опасности за проникване в приложение следствие на пропуски в управлението (препълване на буфер, двойно освобождаване на блок и др). Проектират се и разработват завършени приложения в обектна среда.

**ОПИСАНИЕ НА ДИСЦИПЛИНАТА:** Основни теми: теория и практика на обектното програмиране; декларация и дефиниции на обект, релации между обекти във вертикала и хоризонтала; управление на достъпа до членове на обект; враждане на обекти, приятелски класове, припокриване. Обекти и интерфейси. Софтуерни контракти. Ламбда изрази. Управление на памет при обектно изпълнение, проблеми при препълване, двойно освобождаване и др. Принципи на обектния дизайн. Темите са съпроводени с практически обяснения и реализации на софтуерни приложения от студенти в обектна среда.

**ПРЕДПОСТАВКИ:** Синтез и анализ на алгоритми, Въведение в програмирането, Базови програмни езици.

**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 едночасови писмени текущи оценки в средата и края на семестъра (общо 62%), лабораторни упражнения (18%), курсова работа с две задачи (20%).

**ЕЗИК НА ПРЕПОДАВАНЕ:** български

**ПРЕПОРЪЧИТЕЛНА ЛИТЕРАТУРА:** Stroustrup B., The C++ programming language, Addison-Wesley 1991, Sedgewick R., Algorithms in C v1, v2, v3, Pearson Education Inc, 2002, 1. Petzold Ch., Programming Windows, ninth edd, MS Press 2017, Richter J., Microsoft .NET Framework, SoftPress, 2014, Watkins D., etc, Programming in the .NET Environment, Addison-Wesley, 2016, Deitel P., H. Deytel, C++ Now to program, Pearson 2014

## ХАРАКТЕРИСТИКА НА УЧЕБНАТА ДИСЦИПЛИНА

Наименование на учебната дисциплина: <b>Криптографски методи за защита на информация</b>	Код: <b>BCS06</b>	Семестър: <b>5</b>
Вид на обучението: Лекции (Л) Лабораторни упражнения (ЛУ) Курсова работа (КР) – по избор	Семестриален хорариум: Л – 30 часа ЛУ – 15 часа	Брой кредити: <b>5</b>
Курсов проект (КП) – по избор	Код: <b>BCS07</b>	Брой кредити: <b>2</b>

### ЛЕКТОР(И):

Доц. д-р инж. Антония Ташева (ФКСТ), тел.: 965 2224, e-mail: atasheva@tu-sofia.bg  
ас. Павел Стойнов, pstounov@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 курса е да запознае студентите с основните принципи, заложи в науката *Криптография* и нейното приложение за защита на информацията в съвременните компютърни и комуникационни системи. Получените знания могат да бъдат използвани в практиката за решаване на задачите, свързани с осигуряването на надеждна криптографска защита в различни сфери – комуникация, е-бизнес, мобилно банкиране, системи за електронно разплащане и други.

**ОПИСАНИЕ НА ДИСЦИПЛИНАТА:** Учебният материал включва основни теоретични аспекти на криптографските методи и алгоритми. Основни теми: Въведение в криптографията и история на шифрите; Математически основи на криптографията; Вероятности и случайни числа; Класификация на съвременните алгоритми за криптиране; Хеш функции; Симетрични криптографски алгоритми; Поточни шифри; Асиметрични криптографски алгоритми.; Основи на криптоанализа.

**ПРЕДПОСТАВКИ:** Дисциплината се основава на познания на студентите по математика и същността на компютърните системи и мрежи. Изучени предмети: „Математика“.

**МЕТОД ЗА ПРЕПОДАВАНЕ:** Лекции, изнасяни с помощта на нагледни материали, слайдове в електронен формат, компютър и мултимедиялен прожектор. Лабораторни упражнения, изпълнявани в компютърен учебен клас в екипи, по времето на които се решават практически задачи.

**МЕТОДИ НА ИЗПИТВАНЕ И ОЦЕНЯВАНЕ:** Оценяване по време на лабораторни упражнения и лекции (20%), изпит с теоретични въпроси и практически задачи (80%).

**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. William Easttom, *Modern Cryptography Applied Mathematics for Encryption and Information Security*, Springer, 2021; 4. Craig Bauer, *Secret History: The Story of Cryptology*, Chapman & Hall/CRC Cryptography and Network Security Series, Chapman and Hall/CRC, 2021.

## ХАРАКТЕРИСТИКА НА УЧЕБНАТА ДИСЦИПЛИНА

Наименование на учебната дисциплина: <b>Стандарти за киберсигурност</b>	Код: <b>FaBCS02.1</b>	Семестър: <b>5</b>
Вид на обучението: Лекции (Л) Лабораторни упражнения (ЛУ)	Семестриален хорариум: Л – 30 часа ЛУ – 15 часа	Брой кредити: <b>3</b>

### **ЛЕКТОР(И):**

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

Доц. д-р инж. Кирил Късев (ФТК), тел.: 965 21 34, e-mail: [kmk@tu-sofia.bg](mailto:kmk@tu-sofia.bg)

Технически университет-София

**СТАТУТ НА ДИСЦИПЛИНАТА В УЧЕБНИЯ ПЛАН:** Факултативна 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 концепцията на създаването и прилагането на различни стандартизационни изисквания и добри практики. Ще имат познания за основните групи и типове стандарти в областта на киберсигурността и управлението ѝ.

**ОПИСАНИЕ НА ДИСЦИПЛИНАТА:** По време на курса се изучават: Структура на международните стандарти на International Standards Organization (ISO). Цикъл на Деминг. Подходи за оценка на съответствието на системите с изискванията на стандарта. Планиране, провеждане, докладване и извършване последващи действия от одит. Процесен подход, Принципи за управление на сигурността, Изисквания на ISO. X.800: Security architecture for Open Systems Interconnection for SSITT applications, Регламент (ЕС) 2016/679 на Европейския парламент за защита на физическите лица във връзка с обработването на лични данни. Основни изисквания и рамка за изграждане на система за управление по изискванията на БДС ISO/IEC 27001:2017 Информационни технологии. Методи за сигурност. Системи за управление на сигурността на информацията. Основни изисквания и рамка за изграждане на система за управление по изискванията на БДС ISO/IEC 27701:2020 за управление на неприкосновеността на личната информация. Стандарт PCI DSS - сигурност на данните при електронни карти. Стандартизационна рамка в САЩ в областта на киберсигурността – NIST National Institute of Standards and Technology. Серия от стандарти – 800-XX. Стандарт за информационна и киберсигурност в автомобилната индустрия – TISAX (Trusted Information Security Assessment Exchange). Стандарт ISO 22301:2012, Изисквания към системите за управление на непрекъснатостта на бизнеса. Техники за извършване на одити на системи за управление и системи за сигурност.

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

**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. ISO/IEC 27001 Information technology-Security techniques-Information security management systems-Requirements, 2021; 2. ISO 22301:2019 Security and resilience Business continuity management systems,Requirements, 3: Payment Card Industry Data Security Standard (PCI DSS), 2017; 4. Branden R. Williams, PCI Compliance: Understand and Implement Effective PCI Data Security Standard Compliance, ISBN-10:59749948X, 2017; 5. Introduction to Information Security and ISO 27001, IT Governance Publishing, ISBN-10:1849285268, 2020.

## ХАРАКТЕРИСТИКА НА УЧЕБНАТА ДИСЦИПЛИНА

Наименование на учебната дисциплина: <b>Политики за сигурност и прилагане</b>	Код: <b>FaBCS02.2</b>	Семестър: <b>5</b>
Вид на обучението: Лекции (Л) Семинарни упражнения (СУ) Курсова работа (КР)	Семестриален хорариум: Л – 30 часа СУ – 15 часа	Брой кредити: <b>3</b>

### ЛЕКТОР(И):

Проф. дн Минчо Христов Куминев, тел.: 965 2180, mincho-hristov@tu-sofia.bg  
Гл.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”.

**ЦЕЛИ НА УЧЕБНАТА ДИСЦИПЛИНА:** Целта на учебната дисциплина е да запознае студентите с ролята на сигурността като фактор за развитие на обществото. Разглеждат се различните аспекти на сигурността – национална, международна и глобална, както и методите и структурите, ангажирани с прилагането и. Ролята на конфликтите и тяхното решаване, начини за противодействие на различните видове кризи в обществото, информационните войни, международния тероризъм и други аспекти на сигурността са част от настоящия курс. Специално внимание се отделя на проблемите свързани със сигурността в България - политическа, социална, икономическа.

**ОПИСАНИЕ НА ДИСЦИПЛИНАТА:** Основни теми на курса са: Същност и основни цели на националната сигурност. Глобалното информационно общество и международната сигурност. Специфика на корпоративната сигурност. Международни организации и структури в областта на сигурността. Основни субекти на националната сигурност – външно разузнаване и контраразузнаване. Геополитика и динамика на сигурността. Войни и конфликти в глобалния свят. Международния тероризъм - основни аспекти. Киберсигурност и управление на кризи. Информационни системи за сигурност. Конфликтология, теории на конспирациите и управление на кофликти. Медийни манипулации и информационни войни. Предизвикателства пред националната сигурност на България. Проблеми и перспективи пред Европейската сигурност.

**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:** Денчев, С., Информация и сигурност, С., 2019; Рикардс, Д., След кризата, С., 2020; Христов, М., Аспекти на парламентаризма в системата на българската демокрация, С., 2018; 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; Слатински,Н., Рискът, новото име на сигурността, С., 2019.



## ХАРАКТЕРИСТИКА НА УЧЕБНАТА ДИСЦИПЛИНА

Наименование на учебната дисциплина: <b>Изследвания и анализ на дигитално съдържание</b>	Код: <b>FaBCS02.3</b>	Семестър: <b>5</b>
Вид на обучението: Лекции (Л) Семинарни упражнения (СУ) Текуща оценка (ТО)	Семестриален хорариум: Л – 30 часа СУ – 15 часа	Брой кредити: <b>3</b>

### ЛЕКТОР(И):

доц. д-р Йоана Павлова (СФ), тел.: 965 0878396616, e-mail: ypravlova@tu-sofia.bg  
Технически университет-София

**СТАТУТ НА ДИСЦИПЛИНАТА В УЧЕБНИЯ ПЛАН:** Факултативна 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 разработят методология за подготовка и провеждане на изследвания и да могат да анализират събраните данни. Студентите ще се научат да използват програми за анализ на данни от социални изследвания като SPSS, QDA Miner Lite. .

**ОПИСАНИЕ НА ДИСЦИПЛИНАТА:** Дисциплината „Изследвания и анализ на дигитално съдържание“ цели да запознае студентите с различните видове социални изследвания в интернет среда, тяхната подготовка и провеждане. Курсът ще запознае студентите с основните методи за анализ на данни от социалните изследвания използвайки компютърни програми, които позволяват конструиране на социални индикатори, анализ на връзки и зависимости, и моделиране на социални явления и процеси. Студентите провеждат самостоятелно емпирично изследване и представят анализа на получените резултати в рамките на курса.

**ПРЕДПОСТАВКИ:** Базовите познания от обучението по хуманитарни предмети, статистика. .

**МЕТОД ЗА ПРЕПОДАВАНЕ:** Лекции с използване на слайдове и презентации, семинарни упражнения, където се подготвят различни методи за изследвания, решават се казуси.

**МЕТОДИ НА ИЗПИТВАНЕ И ОЦЕНЯВАНЕ:** Текущата оценки се формира от две писмени работи- тест (30%) и курсова задача-самостоятелно изследване (50%) в края на семестъра, семинарни упражнения (20%).

**ЕЗИК НА ПРЕПОДАВАНЕ:** български

**ПРЕПОРЪЧИТЕЛНА ЛИТЕРАТУРА:** 1. Neuman, W. Lawrence. 2014. Social Research Methods: Qualitative and Quantitative Approaches. Pearson Education, 2. Haralampiev, K., Rabota s Danni v SPSS, Universitetski izdatelstvo “Sv. Kliment Ohridski”, Sofia, 2009. 3. Kalinov, K., Statisticheski metodi v povedencheskite I sotsialnite nauki. Sofia: Nov balgarski universitet, 2001. 4. Naidenova, V., Dzhamdzhieva, M., Staevska, V., Kachestveni metodi v socialnite nauki. Vavedenie. Universitetsko izdatelstvo “Sv. Kliment Ohridski”, Sofia, 2008.

## ХАРАКТЕРИСТИКА НА УЧЕБНАТА ДИСЦИПЛИНА

Наименование на учебната дисциплина: <b>Глобални бази данни</b>	Код: <b>BCS08</b>	Семестър: <b>6</b>
Вид на обучението: Лекции (Л) Лабораторни упражнения (ЛУ) Курсова работа (КР) – по избор	Семестриален хорариум: Л – 30 часа ЛУ – 15 часа	Брой кредити: <b>5</b>
Курсов проект (КП) – по избор	Код: <b>BCS14</b>	Брой кредити: <b>2</b>

### **ЛЕКТОР(И):**

Проф. д-р инж. Даниела Гоцева (ФКСТ), тел.: 965 2328, e-mail: [dgoceva@tu-sofia.bg](mailto:dgoceva@tu-sofia.bg)

Гл. ас. д-р инж. Петко Данов (ФКСТ), тел.: 965 2224, e-mail: [danov@tu-sofia.bg](mailto:danov@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 дисциплината е да запознае студентите с основните концепции при работа с нерелационни бази данни. След успешно завършване на курса студентите трябва да могат да проектират, реализират и използват различни типове нерелационни бази данни.

**ОПИСАНИЕ НА ДИСЦИПЛИНАТА:** Дисциплината разглежда предизвикателствата при работа с големи обеми неструктурирани данни. Представят се основните идеи, залегнали в създаването на различните типове нерелационни бази данни, предимства и недостатъци на различните подходи при работа с тях.

**ПРЕДПОСТАВКИ:** Въведение в програмирането, Базови програмни езици, Платформено-независими програмни езици, Бази данни .

**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. Harrison G. Next Generation Databases: NoSQL and Big Data. Apress, 2015, ISBN: 978-1484213308; 2. Blokdyk G. NoSQL A Complete Guide. 5STARCOOKS, 2021, ISBN: 978-1867320548; 3. Meier A., Kaufmann M. SQL & NoSQL Databases: Models, Languages, Consistency Options and Architectures for Big Data Management. Springer Vieweg, 2019, ISBN: 978-3658245481.

## ХАРАКТЕРИСТИКА НА УЧЕБНАТА ДИСЦИПЛИНА

Наименование на учебната дисциплина: <b>Софтуерни платформи</b>	Код: <b>BCSE09</b>	Семестър: 6
Вид на обучението: Лекции (Л) Лабораторни упражнения (ЛУ) Курсова работа (КР) – по избор	Семестриален хорариум: Л – 30 часа ЛУ – 30 часа	Брой кредити: <b>5</b>
Курсов проект (КП) – по избор	Код: <b>BCSE14</b>	Брой кредити: <b>2</b>

### **ЛЕКТОР(И):**

Проф. д-р инж. Огнян Након Након (ФКСТ), тел.: 965 3613, e-mail: [nakov@tu-sofia.bg](mailto: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 „бакалавър“, специалност “Киберсигурност”, професионално направление 5.3 Комуникационна и компютърна техника, област 5. Технически науки.

**ЦЕЛИ НА УЧЕБНАТА ДИСЦИПЛИНА:** Обучение в модерните технологии за разработка на софтуер. Студентите следва да придобият както теоретична подготовка, необходима им за софтуерни архитекти, така и практически знания за програмиране в среда на Windows, .NET, Visual Studio. Курсът засяга и аспекти на модерното програмиране, валидни за всички съвременни езици и среди, като: обработка на exceptions, управление на памет в многозадачна среда, events – дефиниране и обработка, работа с делегати. Проследява се еволюцията на софтуерните технологии и тенденциите в момента. Разработват се самостоятелно софтуерни приложения в горните среди.

**ОПИСАНИЕ НА ДИСЦИПЛИНАТА:** Основни теми: програмиране в среда на Windows: класически подход, с помощта на класови йерархии, в .NET. Проследява се еволюцията на софтуерните технологии, както и структурното развитие на приложението. Работа със събития: дефиниране, прихващане и обработка; Делегати: предназначение, дефиниране, поглед отвътре и обработка; Управление на памет в многозадачна среда и .NET; Работа с exception в C++ и в .NET – дефиниране, запалване, обработка; сериализация и абстракция на модела; система на общите типове в .NET среда.

**ПРЕДПОСТАВКИ:** Познания по синтеза на алгоритми, познаване на програмните езици C, Java, C++, както и теорията на обектното програмиране. Притежаване на основни практически познания по създаване на софтуер за конзолно приложение.

**МЕТОД ЗА ПРЕПОДАВАНЕ:** Лекции с използване на слайдове и демо-програми, лабораторните упражнения за разработка, компилация и запалване на приложения, протоколи и курсова работа с описание и защита.

**МЕТОДИ НА ИЗПИТВАНЕ И ОЦЕНЯВАНЕ:** изпит с разработка на практическа част и 2 теоретични въпроса, курсова работа с две задачи с възможност за прерастване в реален софтуерен проект, който след успешна защита се признава за изпит.

**ЕЗИК НА ПРЕПОДАВАНЕ:** български

**ПРЕПОРЪЧИТЕЛНА ЛИТЕРАТУРА:** 1. Petzold Ch., Programming Windows, ninth edd, MS Press, 2017; 2. Richter J., Microsoft .NET Framework, SoftPress, 2014; 3. Watkins D., et. al., Programming in the .NET Environment, Addison-Wesley, 2016; 4. Deitel P., H. Deytel, C++ Now to program, Pearson, 2014.

## ХАРАКТЕРИСТИКА НА УЧЕБНАТА ДИСЦИПЛИНА

Наименование на учебната дисциплина: <b>Биометрични системи</b>	Код: <b>BCS10</b>	Семестър: <b>6</b>
Вид на обучението: Лекции (Л) Лабораторни (ЛУ) Курсова работа (КР) – по избор	Семестриален хорариум: Л – 30 часа ЛУ – 15 часа	Брой кредити: <b>5</b>
Курсов проект (КП) – по избор	Код: <b>BCS14</b>	Брой кредити: <b>2</b>

**ЛЕКТОРИ:** доц. д-р Агата Манолова, ФТК, тел:02 9652274, е-мейл: [amanolova@tu-sofia.bg](mailto:amanolova@tu-sofia.bg)  
гл. ас. д-р Никол Христова, ФТК, тел:02 9652274, е-мейл: [nicole.christoff@tu-sofia.bg](mailto:nicole.christoff@tu-sofia.bg)  
гл. ас. д-р Николай Нешов, ФТК, тел:02 9652274, е-мейл: [nneshov@tu-sofia.bg](mailto:nneshov@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 дисциплината е да запознае студентите със системите, използващи биометрична информация, видовете биометрични данни, тяхната обработка и разпознаване, проектиране на биометрични бази данни, моделиране и визуализация на биометрична 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, Математика I, II, III, Сигнали и системи, Базы данни, Основи на предаване на информацията.

**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 упражнения с протоколи.

**МЕТОДИ НА ИЗПИТВАНЕ И ОЦЕНЯВАНЕ:** Оценката се формира от две компоненти: 80% от изпит и 20% от самостоятелна работа, курсова работа, лаб. упражнения.

**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: <b>Сигурни архитектури и протоколи за комуникации</b>	Код: <b>BCS11</b>	Семестър: <b>6</b>
Вид на обучението: Лекции (Л) Лабораторни упражнения (ЛУ) Курсова работа (КР) – по избор	Семестриален хорариум: Л – 30 часа ЛУ – 30 часа	Брой кредити: <b>5</b>
Курсов проект (КП) – по избор	Код: <b>BCS14</b>	Брой кредити: <b>2</b>

### ЛЕКТОР(И):

Доц. д-р инж. Мария Ненова (ФТК), тел.: 965 21 34, e-mail: [mvn@tu-sofia.bg](mailto:mvn@tu-sofia.bg)  
 Доц. д-р инж. Венцислав Трифонов (ФТК), тел.: 965 21 34, e-mail: [vgt@tu-sofia.bg](mailto:vgt@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, съвременните архитектури, принципи и протоколи за изграждане на сигурни комуникационни системи. Те ще знаят как се проектират сигурни архитектури и ще могат да анализират нивото на защита.

**ОПИСАНИЕ НА ДИСЦИПЛИНАТА:** По време на курса се изучават: Принципи за изграждане на сигурни комуникационни и информационни архитектури. Криптиране. Системи със симетрични и публични ключове. Анализ на сигурността на TCP/IP комуникационни протоколи. Протокол IPSec. Принцип на работа. Метод за автентификация. Протоколи SSL и TLS. RADIUS. Принцип на работа. Методи за автентификация, оторизация и контрол на ресурсите. KERBEROS - Архитектура. Методи за автентификация на клиента и сървъра. Принципи за постигане на сигурност. Примерен модел на мрежа защитена с Kerberos. PGP - Архитектура. Методи за автентификация на клиента и сървъра. Принципи за постигане на сигурност. Примерен модел на мрежа защитена с Kerberos. Виртуални частни мрежи. Видове архитектури. Анализ на Open VPN решения. Особенности при инсталиране на различни операционни системи. Конфигуриране на VPN сървър. Методи за автентификация. Видове атаки в комуникационните и информационните мрежи. Системи превенция на интрузия и защитни стени. Методи за детектиране на интрузии чрез сигнатурни анализи. Методи за защита на мрежи чрез SIEM (Security information and event management) анализ. Анализ на интрузионни събития чрез алгоритми с изкуствен интелект. Стандарти за изграждане на сигурни архитектури.

**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 62%), лабораторни упражнения (18%), курсова работа с две задачи (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.

## ХАРАКТЕРИСТИКА НА УЧЕБНАТА ДИСЦИПЛИНА

Наименование на учебната дисциплина: <b>Сигурно системно програмиране</b>	Код: <b>BCS12.1</b>	Семестър: <b>6</b>
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: <b>4</b>
Курсов проект (КП) – по избор	Код: <b>BCS14</b>	Брой кредити: <b>2</b>

### ЛЕКТОР(И):

Проф. д-р инж. Даниела Гоцева (ФКСТ), тел.: 965 2328, e-mail: [dgoceva@tu-sofia.bg](mailto:dgoceva@tu-sofia.bg)

Доц. д-р инж. Явор Томов (ФКСТ), тел.: 965 2224, e-mail: [yavor\\_tomov@tu-sofia.bg](mailto:yavor_tomov@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 даде на студентите фундаментални познания и професионални умения, за да прилагат подходите, методите и средствата за програмиране в реално време като запознае студентите с основите на изграждането и реализацията на основните механизми в програмирането на С на ниско ниво в UNIX подобни системи, особеностите на създаване на процеси и нишки в езика С, работа в мрежов режим на С. В края на обучението си студентът ще: познава вътрешните механизми на UNIX подобни системи; програмира на С под UNIX на ниско ниво; е наясно с основите на мрежовото и многопотоково програмиране на С; прави разлика между процес и нишка и ще ги използва по предназначение.

**ОПИСАНИЕ НА ДИСЦИПЛИНАТА:** Дисциплината създава умения по програмиране на „ниско ниво“, програмиране в реално време, използване на операционни системи с отворен код и създаване на отворено програмно осигуряване.

**ПРЕДПОСТАВКИ:** Знания по програмиране от дисциплините „Базови програмни езици“ и “Операционни системи”.

**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. K.C.Wang, Systems Programming in Unix/Linux, ASpringer1, 1st Ed., 2018. 2. Jin-Jwei Chen, System Programming Vol I and II, jcnh888@gmail.com, 1st Ed., 2020. 3. Sri Manikanta Palakollu, Practical System Programming with C: Pragmatic Example Applications in Linux and Unix-Based Operating Systems, Apress 1st Ed., 2020. 4. Jack-Benny Persson, inux System Programming Techniques: Become a proficient Linux system programmer using expert recipes and techniques, 1st Ed., Packt Publishing, 2021.

## ХАРАКТЕРИСТИКА НА УЧЕБНАТА ДИСЦИПЛИНА

Наименование на учебната дисциплина: <b>Сигурност в кибер физични системи</b>	Код: <b>BCS12.2</b>	Семестър: <b>6</b>
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: <b>4</b>
Курсов проект (КП) – по избор	Код: <b>BCS14</b>	Брой кредити: <b>2</b>

**ЛЕКТОРИ:** проф. д-р Георги Илиев ФТК, тел:029653029, е-мейл: [gli@tu-sofia.bg](mailto:gli@tu-sofia.bg)  
доц. д-р Агата Манолова ФТК, тел:029652274, е-мейл: [amanolova@tu-sofia.bg](mailto:amanolova@tu-sofia.bg)  
гл. ас. д-р Юлиян Велчев ФТК, тел: 02 9652660, е-мейл: [julian\\_s\\_velchev@abv.bg](mailto:julian_s_velchev@abv.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:** В този курс студентите ще научат за основите на кибер физичните системи (КФС), включително принципите на проектиране и методологии. Освен това ще се разгледат подробно предизвикателствата за сигурността на КФС, които се различават на практика поради разнообразния характер на средата на приложение. След успешното завършване на този курс студентите ще могат да: Опишат основния дизайн, архитектурата и принципите на проектиране на КФС; Идентифицират системно източниците на уязвимост в КФС; Определят как сигурността е включена при различни абстракции и при различни компоненти на КФС; Сравняват и съпоставят КФС.

**ОПИСАНИЕ НА ДИСЦИПЛИНАТА:** Основни теми: Въведение в кибер физичните системи (КФС); Атаки и заплахи в КФС; Подобряване на сигурността и поверителността за КФС; Перспективи за сигурност на КФС; КФС Архитектура и атаки; Стратегии за смекчаване на атаки в КФС; Сигурност и поверителност в облачни и вградени системи; Сигурност и поверителност в КФС за големи данни;

**ПРЕДПОСТАВКИ:** Въведение в програмирането, Математика I, II, III, Сигнали и системи, Бази данни, Основи на предаване на информацията; Мрежова сигурност.

**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: Две едночасови писмени текущи оценки в средата и края на семестъра (общо 80%) и 20% от самостоятелна работа, курсова работа, лаб./семинарни упражнения.

**ЕЗИК НА ПРЕПОДАВАНЕ:** български/английски

**ПРЕПОРЪЧИТЕЛНА ЛИТЕРАТУРА:** 1. Y. Maleh, M. Shojafar, A. Darwish, A. Haqiq, *Cybersecurity and Privacy in Cyber Physical Systems*, ISBN 9781138346673, 2019 CRC Press; 2. H. Song, G. A. Fink, S. Jeschke, *Security and Privacy in Cyber-Physical Systems: Foundations, Principles, and Applications*, John Wiley & Sons, 2017, ISBN 9781119226048; 3. A. Awad, S. Furnell, M. Paprzycki, S. K. Sharma, *Security in Cyber-Physical Systems: Foundations and Applications*, Springer, 2021, ISBN 9783030673611; 4. A. Luhach, A. Elçi, *Artificial Intelligence Paradigms for Smart Cyber-Physical Systems*, IGI Global, 2020, ISBN 9781799851028; 5. S. Guo, D. Zeng. *Cyber-Physical Systems: Architecture, Security and Application*, Springer, 2019, ISBN 9783319925639.

## ХАРАКТЕРИСТИКА НА УЧЕБНАТА ДИСЦИПЛИНА

Наименование на учебната дисциплина: <b>Защита на уеб приложения</b>	Код: <b>BCS13.1</b>	Семестър: <b>6</b>
Вид на обучението: Лекции (Л) Лабораторни упражнения (ЛУ) Курсова работа (КР) – по избор	Семестриален хорариум: Л – 30 часа ЛУ – 15 часа	Брой кредити: <b>4</b>
Курсов проект (КП) – по избор	Код: <b>BCS14</b>	Брой кредити: <b>2</b>

### ЛЕКТОР(И):

Проф. д-р инж. Огнян Наков (ФКСТ), тел.: 965 2513, e-mail: [nakov@tu-sofia.bg](mailto:nakov@tu-sofia.bg)  
Ас. маг. инж. Георги Георгиев (ФКСТ), тел.: 965 2224, e-mail: [georgiggeorgiev@tu-sofia.bg](mailto:georgiggeorgiev@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 даде на студентите фундаментални познания и професионални умения в областта на сигурността на уеб приложенията, за да познават и прилагат средствата и методите за проектиране и имплементиране на устойчив за хакерски атаки код в уеб среда. В края на обучението си студентът ще: познава вътрешните механизми и принципите на действие на хакерски атаки от тип SQL инжекция, XSS, DOS и техните разновидности; бъде запознат с приетите добри практики при проектиране на устойчиви за хакерски атаки уеб приложения; може да разпознава и коригира уязвимости към уеб-базирани хакерски атаки в програмен код; познава средства и подходи за автоматизирано тестване и откриване на уязвим код.

**ОПИСАНИЕ НА ДИСЦИПЛИНАТА:** Дисциплината създава умения по идентифициране на уязвимости и проектиране на сигурни уеб приложения.

**ПРЕДПОСТАВКИ:** Знания по програмиране от дисциплината „Базови програмни езици“. Основно разбиране на езиците C#, JavaScript, SQL, markup езици HTML и XML.

**МЕТОД ЗА ПРЕПОДАВАНЕ:** Лекции с използване на слайдове и демо-програми, лабораторни упражнения с работа със специализиран софтуер.

**МЕТОДИ НА ИЗПИТВАНЕ И ОЦЕНЯВАНЕ:** Писмен изпит.

**ЕЗИК НА ПРЕПОДАВАНЕ:** български/английски

**ПРЕПОРЪЧИТЕЛНА ЛИТЕРАТУРА:** 1. Mohd Yunus, Mohd Amin & Brohan, Muhammad & Mohd Nawi, Nazri & Salwana, Ely & Najib, Nurhakimah & Liang, Chan. (2018). Review of SQL Injection : Problems and Prevention. JOIV : International Journal on Informatics Visualization. 2. Kadam, M. & Pradhan, Madhavi & Nalamwar, Sonali. (2011). Security against cross site scripting (XSS) attacks: signature based model on server side. 3. Tripathi, Nikhil & Mehtre, Babu. (2013). DoS and DDoS Attacks: Impact, Analysis and Countermeasures. 4. Pandey, Brijesh & Singh, Alok & Balani, Lovely. (2015). ETHICAL HACKING (Tools, Techniques and Approaches).



## ХАРАКТЕРИСТИКА НА УЧЕБНАТА ДИСЦИПЛИНА

Наименование на учебната дисциплина: <b>Надеждност и безопасност в критични инфраструктури</b>	Код: <b>BCS13.2</b>	Семестър: <b>6</b>
Вид на обучението: Лекции (Л) Лабораторни упражнения (ЛУ) Курсова работа (КР) – по избор	Семестриален хорариум: Л – 30 часа ЛУ – 15 часа	Брой кредити: <b>4</b>
Курсова проект (КП) – по избор	Код: <b>BCS14</b>	Брой кредити: <b>2</b>

### **ЛЕКТОР(И):**

Доц. д-р инж. Ташко Николов (ФТК), тел.: 965 3203, e-mail: [tan@tu-sofia.bg](mailto:tan@tu-sofia.bg)  
Гл. ас. д-р инж. Деница Кирева-Михова (ФТК), тел.: 965 3544, e-mail: [kireva@tu-sofia.bg](mailto:kireva@tu-sofia.bg)  
Технически университет-София

**СТАТУТ НА ДИСЦИПЛИНАТА В УЧЕБНИЯ ПЛАН:** Задължително избираема 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 бъдат запознати с концепциите и етапите на разработка на системи за управление на критични инфраструктури, започвайки от спецификацията им през моделирането, с цел синтез и анализ, и се завърши със сертифицирането им. Ще могат да използват методи и техники за описание на действието и анализ на отказоустойчивостта, както и прилагането им в реални системи.

**ОПИСАНИЕ НА ДИСЦИПЛИНАТА:** Тази дисциплина третира проявленията на случайни, а не на преднамерени, събития в критичните системи. От интерес тук е какво е влиянието на тези събития върху устойчивостта на този вид системи. Основни теми: Основни понятия и концепции за надеждност и безопасност; Безопасност и откзоустойчивост - изисквания, техники и методи за анализ; Функционална безопасност; Влияние на човешкия фактор върху безопасността; Нива на безопасност (SIL); Архитектури на високоотговорни и откзоустойчиви системи; Моделиране и етапи на разработка; Одобрение и сертифициране на високоотговорни системи; Запознаване с реални системи

**ПРЕЛПОСТАВКИ:** Необходими са основни познания по компютърни системи, телекомуникационни или компютърни мрежи, математика и в частност теория на вероятностите.

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

**МЕТОДИ НА ИЗПИТВАНЕ И ОЦЕНЯВАНЕ:** Две едночасови писмени текущи оценки в средата и края на семестъра (общо 62%), лабораторни упражнения (18%), курсова работа (20%).

**ЕЗИК НА ПРЕПОДАВАНЕ:** български

**ПРЕПОРЪЧИТЕЛНА ЛИТЕРАТУРА:** 1. Kai Borgeest. Fundamentals of functional safety. EMC and Functional Safety of Automotive Electronics, 2018; 2. M.S. Carey. Human factors in the design of safety-related systems. Computing & Control Engineering Journal, Volume 11, Issue 1, 2000, p. 28 - 32; 3. Николов, Т., Ал. Ценов, *Моделиране на телекомуникационни процеси и системи*, ЕКС-Либрис ПК, София, 2007; 4. Steven Taylor, Markov Models: An Introduction to Markov Models, CreateSpace Independent Publishing Platform, 2017, SBN:978-1-5484-8455-2

## ХАРАКТЕРИСТИКА НА УЧЕБНАТА ДИСЦИПЛИНА

Наименование на учебната дисциплина: <b>Правни аспекти на киберсигурността</b>	Код: <b>FaBCS03.1</b>	Семестър: <b>6</b>
Вид на обучението: Лекции (Л) Семинарни упражнения (СУ)	Семестриален хорариум: Л – 30 часа СУ – 15 часа	Брой кредити: <b>3</b>

### ЛЕКТОР(И):

Доц. д-р Ралица Димитрова (СФ), тел.: 965 2990, e-mail: [rvd@tu-sofia.bg](mailto:rvd@tu-sofia.bg)

Технически университет-София

**СТАТУТ НА ДИСЦИПЛИНАТА В УЧЕБНИЯ ПЛАН:** Факултативна 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 притежават основни познания за правната уредба на използването на информационните технологии в частния и публичния сектор; да работят с европейски и национални актове в тази област; и да използват познанията си за анализ и решаване на примерни казуси в изучаваната област.

**ОПИСАНИЕ НА ДИСЦИПЛИНАТА:** Основни теми: Електронен документ и електронно изявление; Електронен подпис; Удостоверителни услуги – изисквания към доставчиците, издаване, спиране и прекратяване на удостоверения; Електронна търговия; Услуги на информационното общество – изисквания при сключване на договори чрез електронни средства, режим на търговските съобщения, задължения и отговорност на доставчиците; Защита на интелектуалната собственост в областта на информационните технологии; Защита на потребителите в областта на информационните технологии; Електронна идентификация; Електронно управление.

**ПРЕДПОСТАВКИ:** Познания в областта на информационните технологии, не са необходими предварителни познания в областта на правото.

**МЕТОД ЗА ПРЕПОДАВАНЕ:** Лекции с използване на PowerPoint презентации; по време на семинарните упражнения - анализ на нормативни актове и дела, решаване на тестове и казуси, дискусии по разглежданите теми.

**МЕТОДИ НА ИЗПИТВАНЕ И ОЦЕНЯВАНЕ:** Един писмен тест в средата на семестъра (общо 60%), решаване на казус (20%), активно участие в семинарните упражнения (20%).

**ЕЗИК НА ПРЕПОДАВАНЕ:** български

**ПРЕПОРЪЧИТЕЛНА ЛИТЕРАТУРА:** 1. Колев, Т., Цакова, И. Право и интернет: Въведение в правото и правното регулиране на виртуалното пространство. С., Унив. изд. Св. Климент Охридски, 2015. ISBN 9789540738987; 2. Димитров, Г. Право на информационните и комуникационните технологии Том I. Гражданскоправни аспекти. С., Фондация „Право и интернет“, 2014. ISBN 978-619-7192-06-03; 3. Димитров, Г. Право на информационните и комуникационните технологии Том II. Административноправни и технологични аспекти. С., Фондация „Право и интернет“, 2014; 4. Койчева, Б., Електронната търговия. С., Мартилен, 2014. ISBN 978 954 598 1517; 5. Калайджиев, А., Б. Белазелков, Г. Димитров, М. Йорданова, Д. Марков, В. Станчева. Електронният документ и електронният подпис – правен режим. С., Сиела, 2004. ISBN 954-649-676-6.

## ХАРАКТЕРИСТИКА НА УЧЕБНАТА ДИСЦИПЛИНА

Наименование на учебната дисциплина: <b>Защита на интелектуалната собственост</b>	Код: <b>FaBCS03.2</b>	Семестър: <b>6</b>
Вид на обучението: Лекции (Л) Семинарни упражнения (СУ)	Семестриален хорариум: Л – 30 часа СУ – 15 часа	Брой кредити: <b>3</b>

### **ЛЕКТОР(И):**

Проф. д-р юр. инж. Стефан Стефанов (СФ), тел.: 965 3693, e-mail: [stefanov@tu-sofia.bg](mailto:stefanov@tu-sofia.bg)

Гл. ас. д-р юр. Младен Младенов (СФ), тел.: 965 3693, e-mail: [mladenov@tu-sofia.bg](mailto:mladenov@tu-sofia.bg)

Технически университет-София

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

**ЦЕЛИ НА УЧЕБНАТА ДИСЦИПЛИНА:** Да запознае студентите с необходимите знания относно законодателството в областта на интелектуалната собственост, правната закрила на нейните обекти като нематериални блага и тяхната пазарна реализация чрез осъществяване на ефективна патентно-лицензионна политика в условията на стоково-пазарни отношения и конкуренция.

**ОПИСАНИЕ НА ДИСЦИПЛИНАТА:** Курсът започва с кратко въведение в правото на интелектуалната и индустриална собственост, при което студентите се запознават с неговата същност, функции, основни понятия, система и източници. По-подробно се набляга на:

- създаването и използването на обектите на интелектуалната собственост като изобретения, полезни модели, промишлен дизайн, включително и ноу-хау, в процеса на разработване и внедряване на нови изделия и технологии;
- защита правата на авторите на обекти на индустриална собственост и условията и реда за тяхната правна закрила у нас и в чужбина;
- правно-икономическите резултати от внедряването и използването на нематериалните обекти в производството и тяхната лицензионна реализация като основна форма на технологичен трансфер;

осъществяване на ефективна патентно-лицензионна политика по отношение на националния и международните пазари др.

**ПРЕДПОСТАВКИ:** Не са необходими.

**МЕТОД ЗА ПРЕПОДАВАНЕ:** Лекциите се изнасят с помощта на презентации на powerpoint. В семинарните упражнения се решават правни казуси, извършват се проучвания за ниво на техниката и др.

**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. Закон за патентите и регистрация на полезните модели; 2. Закон за марките и географските означения; 3. Закон за промишления дизайн; 4. Закон за авторското право и сродните му права; 5. Стефанов. Ст.: Международна закрила на полезния модел, ТУ-София, София 2014; 6. Каменова/Стефанов/Кавръкова/Деков: Право на интелектуална собственост, Пловдив 2018.