ХАРАКТЕРИСТИКА НА УЧЕБНАТА ДИСЦИПЛИНА

Наименование на учебната дисциплина: **Електронни доказателства**	Код: **MCSPC01**	Семестър: **3**
Вид на обучението: Лекции (Л) Лабораторни упражнения (ЛУ) Курсова работа (КР) – по избор	Семестриален хорариум: Л – 15 часа ЛУ – 8 часа	Брой кредити: **5**
Курсов проект (КП) – по избор	Код: **MCSPC07**	Брой кредити: **2**

ЛЕКТОР(И):
Д-р Гергана Костова Върбанова, доктор по направление 3.6. Право. Експерт по законоадтелство в сферата на информационните и комуникационните технологии, адвокат. За контакти: тел. 0897872010; g.varbanova@techlaw.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: Знанията и уменията придобити по учебната дисциплина Електронни доказателства създават предпоставки за многостранна реализация на студените в областта на превенцията, разследването на престъпления и правоприлагането, като дава необходимите познания в областта на приложението на електронните доказателства в различните сфери на гражданския и търговски оборот, съдебните производства (наказателно, гражданско и административно) и начина за събиране, представяне и оценка на електронните доказателства.

ОПИСАНИЕ НА ДИСЦИПЛИНАТА: Понятие за електронни доказателства. Исторически предпоставки за възникването. Международни и национални нормативни актове, приложима правна уредба; Видове електронни доказателства; Електронни документи. Електронни документи съдържащи словесно изявление. Електронни документи несъдържащи електронни изявления; Електронен подпис. Видове електронен подпис. Правна стойност на различните видове електронни подписи; Други квалифицирани услуги - електронен времеви печат, електронен печат, други квалифицирани услуги по Регламент (ЕС) №910/2014; Използване на електронни доказателства в гражданското съдопроизводство. Обезпечаване и събиране на електронни доказателства. Представяне и оспорване на електронни доказателства, приложимо право и съдебна практика.

ПРЕДПОСТАВКИ: международните приложими актове и националното законодателство; видовете електронни доказателства и специфичните особености при тяхното използване в гражданското и наказателното съдопроизводство.

МЕТОД ЗА ПРЕПОДАВАНЕ: Лекции, изнасяни с помощта на нагледни материали, слайдове в електронен формат, компютър и мултимедиен прожектор. В лабораторни упражнения се разглеждат реални практически казуси.

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: Авторски електронен учебник на преподавателя, Върбанова, Г. (2020) Правен режим на електронните документи, Данграфик, Варна, Конвенция на Съвета на Европа за престъпленията в кибернетичното пространство, Димитров, Г., Право на информационните и комуникационните технологии, Част първа: Гражданскоправни аспекти, Фондация „Право и интернет“, София, 2014, Димитров, Г., Право на информационните и комуникационните технологии, Част втора: Административноправни и технологични аспекти, Фондация „Право и интернет“, София, 2012

ХАРАКТЕРИСТИКА НА УЧЕБНАТА ДИСЦИПЛИНА

Наименование на учебната дисциплина: **Материално-правни аспекти на компютърните престъпления**	Код: **MCSPC02**	Семестър: **3**
Вид на обучението: Лекции (Л) Лабораторни упражнения (ЛУ) Курсова работа (КР) – по избор	Семестриален хорариум: Л – 15 часа ЛУ – 8 часа	Брой кредити: **5**
Курсов проект (КП) – по избор	Код: **MCSPC07**	Брой кредити: **2**

ЛЕКТОР(И):

Проф. д-р Георги Георгиев Димитров, професор по направление 4.6. Информатика и компютърни науки. Водещ национален експерт по законоадтелство в сферата на информационните и комуникационните технологии, адвокат. За контакти: тел. 0888774666; george.dimitrov@dpc.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: Знанията и уменията по материално-правни аспекти на компютърните престъпления създават предпоставки за многостранна реализация на студените в областта на превенцията, разследването на престъпления и правоприлагането. Курсът запознава студентите с принципите на компютърните престъпления, тяхната специфика от гледна точка на обекта на посегателство, закриляните обществени отношения, като по-специално се разглеждат: видове компютърни престъпления; същински компютърни престъпления; несъщински компютърни престъпления; общи състави; привилегировани състави; квалифицирани състави

ОПИСАНИЕ НА ДИСЦИПЛИНАТА: Основни теми: Понятие за компютърно престъпление като видово понятие на родовото понятие за престъпление. Исторически предпоставки за възникването. Международни и национални нормативни актове,

Видове компютърни престъпления. Същински и несъщински. Отграничение, нормативна техника за регулиране; Нормативни понятия, свързани с компютърните престъпления. Особености и съществени елементи; Същински компютърни престъпления. Общи характерстики относно обект, субект, обективна и субективна страна на престъпленията ; Неактивно хакерство. Основни и квалифицирани състави.

ПРЕДПОСТАВКИ: Превенция на киберпрестъпления, особености на престъпленията от обективна, субективна страна, обекти и наказателно-отговорни лица

МЕТОД ЗА ПРЕПОДАВАНЕ: Лекции, изнасяни с помощта на нагледни материали, слайдове в електронен формат, компютър и мултимедиен прожектор. В лабораторни упражнения се разглеждат реални практически казуси.

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. Авторски електронен учебник на преподавателя - Компютърни престъпления, 2.PPT авторски презентации, 3. Копчева, М., Компютърни престъпления, Сиби, София: 2006, 4.Димитров, Г., Калайджиев, А., Белазелков, Б., Йорданова, М., Станева, В., Марков, Д. Електронният документ и електронният подпис. Правен режим, Сиела/ЦИД, София: 2004, 5.Беленски, Р., Разследване на компютърни престъпления, Сиела, София: 2006 , 6.Владова-Недкова, И., Разследване на компютърни престъпления, Сиела, София: 2003

ХАРАКТЕРИСТИКА НА УЧЕБНАТА ДИСЦИПЛИНА

Наименование на учебната дисциплина: **Разкриване и разследване на киберпрестъпления**	Код: **MCSPC03**	Семестър: **3**
Вид на обучението: Лекции (Л) Лабораторни упражнения (ЛУ) Курсова работа (КР) – по избор	Семестриален хорариум: Л – 15 часа ЛУ – 8 часа	Брой кредити: **5**
Курсов проект (КП) – по избор	Код: **MCSPC07**	Брой кредити: **2**

ЛЕКТОР(И):

Титуляр на учебната дисциплина е д-р Светослав Донов Василев - завеждащ отдел "Киберпрестъпления" в Националната следствена служба и доктор по направление 3.6 Право на Юридическия факултет на Софийския университет „Св. Климент Охридски.
За контакти: тел: 02 / 9069 319, sv.vasilev@nsls.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: Знанията и уменията по разкриване и разследване на киберпрестъпления - практически проблеми създават предпоставки за многостранна реализация на студените в областта на превенцията, разследването на престъпления и правоприлагането. Курсът запознава студентите с основните видове киберпрестъпления, способите за извършването им и практическтите проблеми при разкреването и разследването им. Особено внимание е отделено на използването на открити източници при разследването, както и на практическите проблеми при проследяване на транзакции с криптоактиви и тяхното изземване.

ОПИСАНИЕ НА ДИСЦИПЛИНАТА: Предпоставки за ефективно разследване - предварително обезпечаване, участници и задължения. OSINT; Разкриване и разследване на различни видове измами, престъпления и инциденти, случващи се в социалните мрежи; Разследване на разпространение на порнографски материали. Кибартормоз и връзката му с други престъпления; Интелектуална собственост – основни видове заплахи и киберпрестъпления; Основни предизвикателства пред кибесигурността. Превенция срещу Кибертероризъм; Разследване на атаки срещу компютърни системи и мрежи; Разследване в Даркнет; Проследяване и изземване на криптоактиви; Основни специфики при организиране и изпълнение на претърсване и изземване на доказателства; Експертизи на информационни носители; Осигуряване на цялост и неприкосновенност на данни получени от контрагенти.

ПРЕДПОСТАВКИ: превенцията, разследването на престъпления и правоприлагането

МЕТОД ЗА ПРЕПОДАВАНЕ: Лекции, изнасяни с помощта на нагледни материали, слайдове в електронен формат, компютър и мултимедиен прожектор. В лабораторни упражнения се разглеждат реални практически казуси.

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.Електронен учебник - Методика за разследване на киберпрестъпления - ПБР, 2016г., 2. OSINT techniques, Resourses for Uncovering Online Information, Michael Bazzell, 2023, 3. Digital Evidence and Computer Crime, Third Edition: Forensic Science, Computers and the Internet - Eoghan Casey, Academic Press, 2011, 4. Investigating Cryptocurrencies: Understanding, Extracting, and Analyzing Blockchain Evidence, Nick Furneaux, 2018, John Wiley & Sons, Inc.

ХАРАКТЕРИСТИКА НА УЧЕБНАТА ДИСЦИПЛИНА

Наименование на учебната дисциплина: **Процесуално-правни аспекти на киберпрестъпленията**	Код: **MCSPC04**	Семестър: **3**
Вид на обучението: Лекции (Л) Лабораторни упражнения (ЛУ) Курсова работа (КР) – по избор	Семестриален хорариум: Л – 15 часа ЛУ – 8 часа	Брой кредити: **5**
Курсов проект (КП) – по избор	Код: **MCSPC07**	Брой кредити: **2**

ЛЕКТОР(И):

Титуляр на учебната дисциплина е проф. дюн Георги Иванов Митов - преподавател по наказателен процес (наказателнопроцесуално право) в Юридическия факултет на Софийския университет „Св. Климент Охридски“, За контакти: тел. 02 / 9308 293 mitov@uni-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: Знанията и уменията по процесуално-правни аспекти на киберпрестъпленията създават предпоставки за многостранна реализация на студените в областта на превенцията, разследването на престъпления и правоприлагането. Курсът запознава студентите с принципите на наказателния процес и прилагането им при разследването на киберпрестъпления, тяхната специфика и особености при провеждане на досъдебното производство, както и основните положения при международното сътрудничество по наказателни дела.

ОПИСАНИЕ НА ДИСЦИПЛИНАТА: Основни принципи при разследването на кибепрестъпления. Предпоставки за ефективно разследване - материално обезпечаване, участници и задължения; OSINT – разследване по открити източници; Разкриване и разследване на измами в мрежата; Разследване на разпространение на порнографски материали. Престъпления срещу малолетни и непълнолетни. Кибертормоз и връзката му с други престъпления; Разследване на престъпления срещу интелектуалната собственост; Кибертероризъм и кибервойни; Разследване на атаки срещу компютърни системи и мрежи; Разследване в Даркнет; Разследване на престъпления, свързани с транзакции на криптоактиви. Проследяване и изземване на криптоактиви; Особености при провеждането на оглед, претърсване и изземване; Експертизи на информационни носители; Запазване и получаване на данни от доставчиците на услуги.

ПРЕДПОСТАВКИ: превенцията, разследването на престъпления и правоприлагането

МЕТОД ЗА ПРЕПОДАВАНЕ: Лекции, изнасяни с помощта на нагледни материали, слайдове в електронен формат, компютър и мултимедиен прожектор. В лабораторни упражнения се разглеждат реални практически казуси.

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. Противодействие на организираната престъпност. С.: Прокуратура на Република България, 2013, 608. (Съавт.: Иван Видолов, Ралица Илкова, Десислава Давидкова – Димитрова, Николета Кузманова). 2. Митов, Георги и др. Кратък лекционен курс по Наказателнопроцесуално право / М. Чинова - София, Сиела, 2021. ISBN 978-954-28-3414-4

ХАРАКТЕРИСТИКА НА УЧЕБНАТА ДИСЦИПЛИНА

Наименование на учебната дисциплина: **Видео и аудио анализ в криминалистиката**	Код: **MCSPC05**	Семестър: **3**
Вид на обучението: Лекции (Л) Лабораторни упражнения (ЛУ) Курсова работа (КР) – по избор	Семестриален хорариум: Л – 15 часа ЛУ – 8 часа	Брой кредити: **4**
Курсов проект (КП) – по избор	Код: **MCSPC07**	Брой кредити: **2**

ЛЕКТОР(И):

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 Николай Нешов, ФТК, тел:02 9652274, е-мейл: nneshov@tu-sofia.bg
Технически университет-София

СТАТУТ НА ДИСЦИПЛИНАТА В УЧЕБНИЯ ПЛАН: 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: 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: Въведение в програмирането, Системи за сигурност, Изкуствен интелект и киберсигурност.

МЕТОД ЗА ПРЕПОДАВАНЕ: Лекции с използване на слайдове и демо-програми, 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

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: **Сигурни протоколи и архитектури за комуникации**	Код: **MCSPC06.1**	Семестър: **3**
Вид на обучението: Лекции (Л) Лабораторни упражнения (ЛУ) Курсова работа (КР) – по избор	Семестриален хорариум: Л – 15 часа ЛУ – 8 часа	Брой кредити: **4**
Курсов проект (КП) – по избор	Код: **MCSPC07**	Брой кредити: **2**

ЛЕКТОРИ: доц. д-р Мария Ненова (ФТК), тел.: 965 2134, email: mvn@tu-sofia.bg
проф. д-р Георги Илиев (ФТК), тел. 965 3029, email: gli@tu-sofia.bg
Технически Университет-София

СТАТУТ НА ДИСЦИПЛИНАТА В УЧЕБНИЯ ПЛАН:

Избираема дисциплина за редовни студенти по специалност "Киберсигурност и превенция на киберпрестъпления" за образователно-квалификационната степен "магистър".

ЦЕЛИ НА УЧЕБНАТА ДИСЦИПЛИНА:

Целта на обучението по "Сигурни протоколи и архитектури за комуникации" е студентите да изучат основните методи, принципи и протоколи за изграждане на сигурни комуникационни системи. Да могат да проектират сигурни архитектури и анализират нивото на защита.

ОПИСАНИЕ НА ДИСЦИПЛИНАТА:

По време на курса се изучават основните елементи на сигурността, криптографски методи за защита на данни в компютърни комуникационни мрежи, стандартизирани криптографски алгоритми, квантова криптография, Протокол IPSec (Принцип на работа. Метод за автентификация на пакетите.) Принципите на работа на протоколи SSL и TLS. Протокол RADIUS – конфигуриране, 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. Метод за изграждане на цифровия подпис. Структура на сертификата. Използвани алгоритми за криптиране. Виртуални частни мрежи - видове архитектури, open VPN. Изучват се особеностите при инсталирането на различни операционни системи. Конфигуриране на VPN сървър. Методи за автентификация.

ПРЕДПОСТАВКИ: Необходими са основни познания по операционни системи, основи на мрежовите технологии, комуникационни мрежи, предаване на данни и компютърни комуникации.

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. Ch. Brooks, Ch. Grow, Ph. Craig, D. Short, Cyber Security Essentials, Sibex, ISBN-10: 9781119362395, 2018. **2.** C. Dotson, Practical Cloud Security: A Guide for Secure Design and Deployment 1st Edition, O'Reilly Media, ISBN-10: 1492037516, 2019. **3.** Pascal Ackerman, Industrial Cybersecurity: Efficiently secure critical infrastructure systems, Packt Publishing, ISBN-10: 1788395158, 2017. **4.** Stallings W., Cryptography and Network Security: Principles and Practice, 5/E, Prentice Hall, ISBN-10: 0134444280, 2016. **5.** Elbirt A., Applied Cryptography: Protocols, Algorithms and Source Code in C 20th Edition, Publisher: Wiley; 20 edition, ISBN-10:1119096723, 2015.

ХАРАКТЕРИСТИКА НА УЧЕБНАТА ДИСЦИПЛИНА

Наименование на учебната дисциплината: **Облачни технологии**	Код: **MCSPC06.2**	Семестър: **3**
Вид на обучението: Лекции (Л) Лабораторни упражнения (ЛУ) Курсова работа (КР) – по избор	Семестриален хорариум: Л – 15 часа ЛУ – 8 часа	Брой кредити: **4**
Курсов проект (КП) – по избор	Код: **MCSPC07**	Брой кредити: **2**

ЛЕКТОР:

Доц. д-р инж. Даниела Минковска (ФКСТ), тел.: 9653317, email: daniela@tu-sofia.bg

Технически университет – София

СТАТУТ НА ДИСЦИПЛИНАТА В УЧЕБНИЯ ПЛАН: Избираема дисциплина за редовни студенти по специалност „Киберсигурност и превенция на киберпрестъпления“ на факултет „Компютърни системи и технологии“, за образователно-квалификационната степен „магистър“.

ЦЕЛИ НА УЧЕБНАТА ДИСЦИПЛИНА: Основна цел на дисциплината е да даде фундаментални понятия за облачните технологии, платформи, услуги и архитектури, виртуализация, основните концепции на публичните облачни услуги IaaS, PaaS и SaaS, и приложението им в публични облачни платформи. След завършване на курса студентите трябва да могат да познават съществуващи решения в облачните технологии, да разграничават опциите за съхранение в облак и да описват ресурсите за управление на облак.

ОПИСАНИЕ НА ДИСЦИПЛИНАТА: Изучават се основните понятия, характеристики и услуги в облачните технологии, архитектури на основни платформи за облачни изчисления и облачни операционни системи. Разглеждат се възможностите за виртуализация – видове, клъстерни и GRID технологии. Изучават се методи за управление на паметта, безопастност и защита при работа с облачните технологии. Лабораторните упражнения подпомагат практическото усвояване на материала в съвременни облачни платформи. Курсовата работа включва разработка на съдържателна и презентационнна част, осигуряваща експозиция на научни изследвания в облачните технологии..

ПРЕДПОСТАВКИ: Курсът се базира на получените знания в курсовете по **“**WEB базирани технологии“, **“**Разпределени системи“ и **“**Компютърни мрежи“ от бакалавърската и магистърската степени.

МЕТОД ЗА ПРЕПОДАВАНЕ: Лекции, изнасяни с помощта на нагледни материали, слайдове в електронен формат, компютър и мултимедиен прожектор. Лабораторни упражнения в облачна среда Windows Azure и Amazon Web Services (AWS). Курсов проект – проектиране и изграждане на облачно приложение.

МЕТОДИ НА ИЗПИТВАНЕ И ОЦЕНЯВАНЕ: Текуща оценка

ЕЗИК НА ПРЕПОДАВАНЕ: Български

ПРЕПОРЪЧИТЕЛНА ЛИТЕРАТУРА: 1. Cloud Computing Bible. Barrie Sosinsky. John Wiley & Sons. ISBN-13: 978-0470903568. Amazon Web Services For Dummies. Bernard Golden. For Dummies. ISBN-13: 978-1118571835; 2. Weinhardt, C., Anandasivam, A., Blau, B., Borissov, N., Meinl, T., Michalk, W., Stößer, J.: Cloud Computing – A Classification, Business Models, and Research Directions. Bus. Inf. Syst. Eng. 1, 391–399 (2009); 3. Malathi, M.: Cloud computing Concepts. In: 2011 3rd International Conference on Electronics Computer Technology (ICECT), pp. 236–239 (2011); 4. Gautam Shroff, “Enterprise Cloud Computing Technology Architecture Applications”, Cambridge University Press; 1 edition, [ISBN: 978-0521137355], 2010; 5. Toby Velte, Anthony Velte, Robert Elsenpeter, “Cloud Computing, A Practical Approach” McGraw-Hill Osborne Media; 1 edition [ISBN: 0071626948], 2009; 6. Greg Schulz, “Cloud and Virtual Data Storage Networking”, Auerbach Publications [ISBN: 978-1439851739], 2011; 7. Ronald L. Krutz, Russell Dean Vines, “Cloud Security” [ISBN: 0470589876], 2010; 8. John Rittinghouse, James Ransome, “Cloud Computing” CRC Press; 1 edition [ISBN: 1439806802], 2009; 9. Massimo Cafaro (Editor), Giovanni Aloisio (Editor), “Grids, Clouds and Virtualization” Springer; edition [ISBN: 978-0857290489] 2011; 10. LatifaBoursas (Editor), Mark Carlson (Editor), Wolfgang Hommel (Editor), Michelle Sibilla (Editor), KesWold (Editor), “Systems and Virtualization Management: Standards and New Technologies” [ISBN: 978-3540887072], October 14, 2008.

ХАРАКТЕРИСТИКА НА УЧЕБНАТА ДИСЦИПЛИНА

Наименование на учебната дисциплина: **Мениджмънт на проекти в ИКТ**	Код: **FaMCSPC01**	Семестър: **1**
Вид на обучението: Лекции (Л) Семинарни упражнения (СУ)	Семестриален хорариум: Л – 15 часа СУ – 8 часа	Брой кредити: **3**

ЛЕКТОР(И):

доц. д-р инж. Върбинка Стефанова-Стоянова (ФКСТ), тел.: 965 32 85, e-mail: vvstoyanova@tu-sofia.bg

Технически университет-София

СТАТУТ НА ДИСЦИПЛИНАТА В УЧЕБНИЯ ПЛАН: Факултативна 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: Формиране на теоретични и практически знания и умения за решаване на проблеми, възникнали при управлението на проекти. Развитие на теоретични и практически умения за ефективно управление в сектор ИКТ, включително използването на автоматизирани системи (AMS), осигуряващи постиганетона резултатите, определени в проекта, относно състава и обхвата на работа, разходите, времето, качеството и удовлетвореността на участниците в проекта..

ОПИСАНИЕ НА ДИСЦИПЛИНАТА: Основни теми: „Същност на управлението на проекти“: Характеристики на проектите. Дърво на решенията. „Методи за оценка, основани на мултиплициращи критерии. Рамки за оценка и подбор. „Структуриране на проекта. Организационна структура и структура на разпределяне на задачите“: Организационни структури. Организационна структура на проекта. Съчетаване на организационната структура със структурата на разпределение на дейностите. „Технологичен аспект: избор на конфигурацията, управление и контрол“: Технологични, функционални, качествени и рискови съображения. Конкурентен инженеринг и конкуренция във времето. Управление на риска. TQM, „Планиране на проекти“: Work Breakdown Structure. Диаграма на GANTT. Подход на линейно програмиране при CPM-анализ. Работа при условия на несигурност. PERT-анализ и CPM-допускания. Проектиране на софтуер за управление

ПРЕДПОСТАВКИ: Учебната дисциплина се базира на знания на студентите по микроикономика, управление, математически анализ, теория на вероятностите и математическа статистика, теоретични основи на компютърните науки, корпоративна архитектура, компютърни системи, мрежи, телекомуникации, информационни системи за управление на IT компания.

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

МЕТОДИ НА ИЗПИТВАНЕ И ОЦЕНЯВАНЕ: Дисциплината приключва с **текуща оценка** и оценката се формира от две съставки: : Две едночасови писмени контролни работи в средата и края на семестъра..

ЕЗИК НА ПРЕПОДАВАНЕ: български

ПРЕПОРЪЧИТЕЛНА ЛИТЕРАТУРА: KATHY SCHWALBE., Technology Project Management , 2020., HAROLD KERZNER., Project Management Case Studies., DARRON CLARK, All-In-One PMP® EXAM PREP Kit,1300 Question, Answers, and Explanations, 240 Plus Flashcards,

ХАРАКТЕРИСТИКА НА УЧЕБНАТА ДИСЦИПЛИНА

Наименование на учебната дисциплина: **Политики за киберсигурност**	Код: **MCSPC08**	Семестър: **4**
Вид на обучението: Лекции (Л) Лабораторни упражнения (ЛУ) Курсова работа (КР),	Семестриален хорариум: Л – 15 часа ЛУ – 8 часа	Брой кредити: **3**

ЛЕКТОР(И):

Титуляр на учебната дисциплина е доц. д-р инж. Иван Станков, с научна специалност "Автоматизирани системи за обработка на информация и управление". За контакти: тел. 9652682 mail: istankov@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: Дисциплината създава условия за теоретично и приложно изучаване на проблемите свързани с изготвянето и прилагането на политики за киберсигурност. Студентите ще придобият знание в посока за изучаване на европейски и национални документи, изискващи изготвянето на такива политики. Включени са теоретични и практически аспекти на необходимостта от изготвянето им, като се разглеждат въпроси свързани с теория, формални модели и практико-приложни аспекти на тяхната структура и съдържание.

ОПИСАНИЕ НА ДИСЦИПЛИНАТА: Учебният материал включва основни теоретични аспекти на политиките за киберсигурност. Основни теми: Стратегия за киберсигурност на Европейския съюз; Директиви и регламенти. ENISA (Агенцията на Европейския съюз за киберсигурност) и сертифицирането на киберсигурността на информационните и комуникационните технологии.); Актуализирана национална стратегия на РБългария "Киберустойчива България 2023"; Закон за киберсигурност; Наредба за минималните изисквания за мрежова и информационна сигурност; Управление на МИС; Политика за сигурност; Анализ, оценка и управление на риска за киберсигурността; Управление на инциденти в киберсигурността.

ПРЕДПОСТАВКИ: наредби, регламенти на ЕС разработени политики за управление на киберсигурността, както на национално ниво, така и на международно

МЕТОД ЗА ПРЕПОДАВАНЕ: Лекции, изнасяни с помощта на нагледни материали, слайдове в електронен формат, компютър и мултимедиен прожектор. В лабораторни упражнения се разглеждат реални практически казуси.

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. Network Security Discovering the Optimal & Secure Path by Vulnerability Analysis in Dynamic Network Through Attack Graphs, Gouri R. Patil, |Jul 18, 2022, 2. Vulnerability Analysis A Complete Guide, 2020 Edition, Gerardus Blokdyk, Apr 21, 2021, 3. Vulnerability Analysis and Risk Assessment: For Dynamic Nonmotorized Human Travel Activity Networks, Daniel Kwon, Venky Shankar, Paperback – 26 Feb. 2014, 4. Building Information Systems in the Overall Risk and Security Management in Them, Ivan Stankov, Technical University – Sofia publishing 2021

ХАРАКТЕРИСТИКА НА УЧЕБНАТА ДИСЦИПЛИНА

Наименование на учебната дисциплина: **Защита на уеб приложения**	Код: **MCSPC09**	Семестър: **4**
Вид на обучението: Лекции (Л) Лабораторни упражнения (ЛУ) Курсова работа (КР),	Семестриален хорариум: Л – 15 часа ЛУ – 8 часа	Брой кредити: **3**

ЛЕКТОР(И):
Проф. д-р инж. Огнян Наков (ФКСТ), тел.: 965 2513, e-mail: nakov@tu-sofia.bg
Ас. маг. инж. Георги Георгиев (ФКСТ), тел.: 965 2224, e-mail: georgiggeorgiev@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 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 тестиране 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: текуща оценка.

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: **Сигурност при изграждане и управление на информационни системи и мрежи**	Код: **MCSPC10**	Семестър: **4**
Вид на обучението: Лекции (Л) Лабораторни упражнения (ЛУ) Курсова работа (КР)	Семестриален хорариум: Л –15 часа ЛУ – 15часа	Брой кредити: **3**

ЛЕКТОР(И):

Доц. д-р инж. Иван Станков тел.: 965 2682, e-mail: istankov@tu-sofia.bg
Доц. д-р инж. Върбинка Стефанова- Стоянова (ФКСТ), тел.: 965 30 91, 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 „Сигурност при изграждане и управление на информационни системи и мрежи“ е да предостави на студентите практическо и научно – изследователски знания и опит в сферата на ефективно изграждане и цялостно управление информационни системи и мрежи в работните и съпътстващите процеси.

ОПИСАНИЕ НА ДИСЦИПЛИНАТА: Основни теми: Информационна система. Етапи на изграждане. Видове информационни системи. Основни компоненти и възможности на бизнес интелигентните информационни системи. Моделиране, анализ и управление на бизнес процеси. Международни стандарти за управление на риск и сигурността. PCI DSS, HIPAA и GDPR. Одит на информационни системи. Информационна сигурност. Контроли. Криптиране и одит на информационни технологии. Одит за логическа сигурност. CTI. IAM. Защита и сигурност на крайните точки. SIEM.

ПРЕДПОСТАВКИ: Информационни системи, бизнес управление и организация на фирмена дейност, 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: Изпит(общо 90%) и лабораторни упражнения (10%).

ЕЗИК НА ПРЕПОДАВАНЕ: български

ПРЕПОРЪЧИТЕЛНА ЛИТЕРАТУРА: И. Станков, Изграждане на информационни системи при цялостно управление на риска и сигурността в тях, издателство на Технически университет София 2021;, International Technical Support Organization: www.redbooks.ibm.com; Certified Internet Audit Professional (CIAP), International Computer Auditing Education Association (ICAEA), Й. Хаджийска, Информационни системи, Издателство „За буквите – О писменехъ“ 2014, ISBN 978-619-185-112-6

ХАРАКТЕРИСТИКА НА УЧЕБНАТА ДИСЦИПЛИНА

Наименование на учебната дисциплина: **Етично хакерство**	Код: **MCSPC11**	Семестър:**4**
Вид на обучението: Лекции (Л) Лабораторни упражнения (ЛУ) Курсова работа (КР)	Семестриален хорариум: Л – 15 часа ЛУ – 8 часа	Брой кредити:**3**

ЛЕКТОР(И):
Доц. д-р Явор Томов (ФКСТ), тел.: 02 965-2606, e-mail: yavor_tomov@tu-sofia.bg
ас. маг. 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 „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 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 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 упражнения се провеждат в специализирани лаборатории.

МЕТОДИ НА ИЗПИТВАНЕ И ОЦЕНЯВАНЕ: текуща оценка.

ЕЗИК НА ПРЕПОДАВАНЕ: български/английски

ПРЕПОРЪЧИТЕЛНА ЛИТЕРАТУРА:
1.Daniel G. Graham, Ethical Hacking: A Hands-on Introduction to Breaking In, ISBN 9781718501874, 2021; 2.Tabassum, Mujahid & Sharma, Tripti & Mohanan, Saju. (2021). Ethical Hacking and Penetrate Testing using Kali and Metasploit Framework. 2. 9 -22; 3.Thomas, G. A (2017) “An ethical hacker can help you beat a malicious one”, The Conversation; 4.Thomas G, Low G, Burmeister O (2018) “Who Was That Masked Man?”: System Penetrations—Friend or Foe? In: Prunckun H. (Eds) Cyber Weaponry. Advanced Sciences and Technologies for Security Applications. Springer, Cham; 5.Verizon (2017). “Verizon Data Breach Investigations Report 2017”; 6.Verizon (2018). “Verizon Data Breach Investigations Report 2018”; 7. Mansfield-Devine, S (2017). Hiring ethical hackers: the search for the right kinds of skills. Computer Fraud & Security, 2017(2), 15–20. doi:10.1016/s1361-3723(17)30016-7; 8. Hatfield, J. M. (2019). Virtuous human hacking: The ethics of social engineering in penetration-testing. Computers & Security, 83, 354-366; 9. Sönmez, F. Ö. (2019). Security Qualitative Metrics for Open Web Application Security Project Compliance. Procedia Computer Science, 151, 998-1003; 10. Zabicki, R., & Ellis, S. R. (2017). Penetration Testing. In Computer and Information Security Handbook (pp. 1031- 1038). Morgan Kaufmann; 11. Abraham K White, Hacking: The Underground Guide to Computer Hacking, 2020; 12. Daniel Regalado, Shon Harris, Allen Harper, Gray Hat Hacking: The Ethical Hacker's Handbook, Fifth Edition 5th Edition, ISBN: 9781260108422, 2018; 13. Александър Цокев, Етично хакерство,2017.

ХАРАКТЕРИСТИКА НА УЧЕБНАТА ДИСЦИПЛИНА

Наименование на учебната дисциплина: **Специални разузнавателни средства – оперативен и правен аспект**	Код: **MCSPC12.1**	Семестър: **4**
Вид на обучението: Лекции (Л) Лабораторни упражнения (ЛУ) Курсова работа (КР)	Семестриален хорариум: Л – 15 часа ЛУ – 8 часа	Брой кредити: **3**

ЛЕКТОР(И):

Проф. д-р инж. Иво Великов, тел.: 0887 693411, email: manoflight@abv.bg ВСУ „Черноризец Храбър“ и Държавна комисия по сигурността на информацията

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

ЦЕЛИ НА УЧЕБНАТА ДИСЦИПЛИНА: Дисциплината има за цел обучаваните да получат знания за ролята, предназначението и организацията на използване на Специални разузнавателни средства (СРС) при разкриване на посегателства срещу националната сигурност и обществен ред. Акценти в съдържанието са правно-нормативната уредба на дейността, в контекста на общественото внимание и ограничаването на права при използване на СРС, а също и като високоспециализирана дейност на ограничен кръг държавни служители в службите за сигурност (ДАТО и ДАНС).

ОПИСАНИЕ НА ДИСЦИПЛИНАТА: Съдържанието на дисциплината е изградено на основата на принципа “от общото към частното”, като в първите лекции са застъпени въпроси относно основните права на човека и тяхното ограничаване, основите на използване на СРС, историческо развитие на обществените отношения у нас и в други държави по тази чувствителна за демокрацията тема. В следващите лекции чрез комбиниране на нормативна част и практическа дейност се разкрива организацията на използването на СРС в нашата страна.

ПРЕДПОСТАВКИ: Предполага се, че студентите имат вече подготовка по дисциплините Електронни доказателства, Материалноправна страна на киберпрестъпленията, Процесуалноправни аспекти на киберпрестъпленията, Електронни системи за сигурност...

МЕТОД ЗА ПРЕПОДАВАНЕ: Лекции, изнасяни с помощта на презентации и медиен проектор, флипчарт и бяла дъска, 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 придобият реални представи за тази прецизно и строго регламентирана дейност.

МЕТОДИ НА ИЗПИТВАНЕ И ОЦЕНЯВАНЕ изпит

ЕЗИК НА ПРЕПОДАВАНЕ: български

ПРЕПОРЪЧИТЕЛНА ЛИТЕРАТУРА:

1. БОЙЧЕВ П. ТЕХНИЧЕСКО РАЗУЗНАВАНЕ, “АЛБАТРОС”, СОФИЯ 2003. 2. САВОВ, И., СДОТО, ВУСИ, ПЛОВДИВ 2019 Г. 3. ЕВРОПЕЙСКА КОНВЕНЦИЯ ЗА ПРАВАТА НА ЧОВЕКА. 4. СМЕДОВСКА-ТОНЕВА, Р., СПЕЦИАЛНИ МЕТОДИ ЗА БОРБА С ОРГАНИЗИРАНАТА ПРЕСТЪПНОСТ – АГЕНТИ ПОД ПРИКРИТИЕ, РИСК – МОНИТОР, 2011 Г. 5. САВОВ, И., ВЪЗМОЖНОСТИ ЗА ОПРЕДЕЛЯНЕ НА МЕСТОПОЛОЖЕНИЕТО НА ЧОВЕК ПО НОМЕРА НА МОБИЛНОТО УСТРОЙСТВО, ГОДИШНИК НА ФАКУЛТЕТ ТЕХНИЧЕСКИ НАУКИ, УНИВЕРСИТЕТСКО ИЗДАТЕЛСТВО „ЕПИСКОП КОНСТАНТИН ПРЕСЛАВСКИ“, ШУМЕН, 2020, СТР. 247 – 256, ISSN 1311-834X ; 6. ИЛИН САВОВ, НЯКОИ ПРОЦЕДУРИ ПРИ ЕЛЕКТРОННОТО НАБЛЮДЕНИЕ НА ЧУЖДИ РАЗУЗНАВАНИЯ В СЪЕДИНЕНИТЕ АМЕРИКАНСКИ ЩАТИ, ГОДИШНИК, УНИВЕРСИТЕТСКО ИЗДАТЕЛСТВО „ЕПИСКОП КОНСТАНТИН ПРЕСЛАВСКИ“, ШУМЕН, 2020, СТР. 234-246, ISSN1311-834; (ВИДИМ В ИНТЕРНЕТ) 7. ВЛАДИМИРОВ, ВЛ., ОПЕРАТИВНО-ТЕХНИЧЕСКИ МЕРОПРИЯТИЯ, СВЪРЗАНИ С ПРИЛАГАНЕ НА СРС, АМВР, 2008 Г., ДЕКЛАСИФИЦИРАНО; 8. НИКОЛОВ, Н., СРС В ОПЕРАТИВНО-ИЗДИРВАТЕЛНАТА ДЕЙНОСТ НА ОРГАНИТЕ НА МВР, ВИПОНД - МВР, 1999 Г., ДЕКЛАСИФИЦИРАНО. 9. ГОДИШНИ ДОКЛАДИ НА НБКСРС ЗА ИЗВЪРШЕНАТА ДЕЙНОСТ (ОТ ПРЕДХОДНА ГОДИНА), САЙТ НА БЮРОТО, ВИДИМ В ИНТЕРНЕТ, HTTPS://WWW.NBKSRS.BG/MEDIA/1125/D2019.PDF

НОРМАТИВНИ АКТОВЕ: НАКАЗАТЕЛЕН КОДЕКС; НАКАЗАТЕЛНОПРОЦЕСУАЛЕН КОДЕКС; ЗАКОН ЗА МИНИСТЕРСТВО НА ВЪТРЕШНИТЕ РАБОТИ (ЗМВР); ЗАКОН ЗА СПЕЦИАЛНИТЕ РАЗУЗНАВАТЕЛНИ СРЕДСТВА (ЗСРС); ЗАКОН ЗА ДАНС; ЗАКОН ЗА ЕЛЕКТРОННИТЕ СЪОБЩЕНИЯ (ЗЕС); •НАРЕДБА ЗА ОРГАНИЗАЦИЯТА НА ДЕЙНОСТТА ПО ИЗПОЛЗВАНЕ НА СЛУЖИТЕЛИ ПОД ПРИКРИТИЕ В МИНИСТЕРСТВОТО НА ВЪТРЕШНИТЕ РАБОТИ, В СИЛА ОТ 15.09.2015 Г., ПРИЕТА С ПМС № 247 ОТ 10.09.2015 Г., ОБН. ДВ. БР.71 ОТ 15 СЕПТЕМВРИ 2015Г.

ХАРАКТЕРИСТИКА НА УЧЕБНАТА ДИСЦИПЛИНА

Наименование на учебната дисциплина: **Правни аспекти на защитата на информацията**	Код: **MCSPC12.2**	Семестър: **4**
Вид на обучението: Лекции (Л) Лабораторни упражнения (ЛУ) Курсова работа (КР)	Семестриален хорариум: Л – 15 часа ЛУ – 8 часа	Брой кредити: **3**

ЛЕКТОР(И):

Проф. д-р инж. Иво Великов, тел.: 0887 693411, email: manoflight@abv.bg ВСУ „Черноризец Храбър“ и Държавна комисия по сигурността на информацията

СТАТУТ НА ДИСЦИПЛИНАТА В УЧЕБНИЯ ПЛАН: Свободно избираема дисциплина от учебния план за обучение на студенти по специалност “Киберсигурност и превенция на киберпрестъпления“, на Факултет КСТ на Технически Университет – София за образователно-квалификационна степен “магистър”.

ЦЕЛИ НА УЧЕБНАТА ДИСЦИПЛИНА: Дисциплината има за цел обучаваните да получат знания за нормативната основа, системите от органи и системите от мерки в областта на защитата на информацията, професионалната терминология и конституционно определените права на гражданите в информационната област.

ОПИСАНИЕ НА ДИСЦИПЛИНАТА: Обект на дисциплината са класифицираната информация (КИ), обществената информация (ОИ) и личните данни (ЛД), съобразно българските закони – ЗЗКИ, ЗДОИ и ЗЗЛД. Предмет на учебната дисциплина е системата от органи и системата от мерки, механизми и процедури, предназначени за защита на класифицираната информация, обществената информация и личните данни. Съществена част от предмета на дисциплината е правната регламентация на регулиране на обществените отношения, свързани със създаването, обработването и съхраняването на класифицирана информация, обществена информация и лични данни, както и условията, и реда за предоставяне на достъп до тях.

ПРЕДПОСТАВКИ: Предполага се, че студентите имат вече подготовка по дисциплините Електронни доказателства, Материалноправна страна на киберпрестъпленията, Процесуалноправни аспекти на киберпрестъпленията, Електронни системи за сигурност...

МЕТОД ЗА ПРЕПОДАВАНЕ: Лекции, изнасяни с помощта на презентации и медиен проектор, флипчарт и бяла дъска, 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 придобият практически умения в областта на защитата на информацията.

МЕТОДИ НА ИЗПИТВАНЕ И ОЦЕНЯВАНЕ изпит

ЕЗИК НА ПРЕПОДАВАНЕ: български

ПРЕПОРЪЧИТЕЛНА ЛИТЕРАТУРА: 1. ЗАКОН ЗА ДОСТЪП ДО ОБЩЕСТВЕНА ИНФОРМАЦИЯ, ОБН.ДВ. БР.55/07.07.2000. 2. ЗАКОН ЗА ЗАЩИТА НА КЛАСИФИЦИРАНАТА ИНФОРМАЦИЯ, ОБН. ДВ. БР.45/30.04.2002. 3. ЗАКОН ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ, ОБН. ДВ. БР.1/04.01.2002. 4. ПЪРВОНАЧАЛНО ОБУЧЕНИЕ - СБОРНИК ЛЕКЦИИ, ДЪРЖАВНАТА КОМИСИЯ ПО СИГУРНОСТТА НА ИНФОРМАЦИЯТА, СОФИЯ, 2020. HTTP://WWW.DKSI.BG/NR/RDONLYRES/16DE6365-52E4-4F1F-9D20- E517E74A5BD5/0/SBORNIK_LEKCII_2_2020.PDF