И К О Н О М И Ч Е С К И У Н И В Е Р С И Т Е Т - В А Р Н А

Ц Е Н Т Ъ Р З А М А Г И С Т Ъ Р С К О О Б У Ч Е Н И Е

К А Т Е Д Р А „И Н Ф О Р М А Т И К А“

Приета от ФС (протокол №8 / 05.03.2020 г.) **УТВЪРЖДАВАМ:**

Приета от КС (протокол №7 / 28.02.2020 г.) **Декан:**

(проф. д-р Владимир Сълов)

У Ч Е Б Н А П Р О Г Р А М А

ПО ДИСЦИПЛИНАТА: „КИБЕРСИГУРНОСТ”;

ЗА СПЕЦ: „Информационен мениджмънт в бизнеса“; ОКС „магистър“

КУРС НА ОБУЧЕНИЕ: 5 - СС и СНУ, 6 - СПН и ДНДО;

СЕМЕСТЪР: 10 - СС и СНУ, 11 - СПН и ДНДО;

ОБЩА СТУДЕНТСКА ЗАЕТОСТ: 210 ч.; в т.ч. аудиторна 60 ч.

КРЕДИТИ: 7

РАЗПРЕДЕЛЕНИЕ НА СТУДЕНТСКАТА ЗАЕТОСТ СЪГЛАСНО УЧЕБНИЯ ПЛАН

ВИД УЧЕБНИ ЗАНЯТИЯ	***ОБЩО (часове)***	***СЕДМИЧНА НАТОВАРЕНОСТ (часове)***
АУДИТОРНА ЗАЕТОСТ: т. ч.		
• ЛЕКЦИИ	30	2
• УПРАЖНЕНИЯ (семинарни занятия/ лабораторни упражнения)	30	2
ИЗВЪНАУДИТОРНА ЗАЕТОСТ	150	-

Изготвили програмата:

1. ……..
(доц. д-р Силвия Парушева)

2. ……..
(гл. ас. д-р Михаил Радев)

Ръководител катедра: ……..
„Информатика“ (проф. д-р Юлиан Василев)

I. А Н О Т А Ц И Я

Дисциплината "Киберсигурност" има за цел за предостави на студентите теоретични знания и практически умения относно основите на киберсигурността.

Основните акценти при обучението се поставят върху следните направления:

- *запознаване с важността на киберсигурността за бизнеса и обществото, нейната ключова терминология и основни концепции;*
- *получаване на знания за различните типове хакерски техники за атаки и източниците на заплахи;*
- *овладяване на знания относно превантивните мерки и начините за защита срещу основните типове атаки;*
- *разграничаване на системната и уеб сигурността и техните специфики;*
- *придобиване на способности за прилагане на техники за анализ и ефективна кибер защита.*

Чрез обучението по дисциплината се създават умения за практическо приложение на теоретичните знания и подготовката на студентите за работа в областта на анализите, администрирането и одитирането на киберсигурността и нейната успешна защита.

Дисциплината способства за развитие на способности на студентите за самообучение, работа в екип, за продължаващо обучение и формиране на нови умения, за вземане на решения относно разработване и прилагане в действие на подходящи кибер стратегии.

II. Т Е М А Т И Ч Н О С Ъ Д Ъ Р Ж А Н И Е

No. по ред	НАИМЕНОВАНИЕ НА ТЕМИТЕ И ПОДТЕМИТЕ	БРОЙ ЧАСОВЕ		
		Л	СЗ	ЛУ
Тема 1. Основи на киберсигурността		**4**	**2**	
1.1	Ключова терминология в киберсигурността. Значение на киберсигурността.	2	2	
1.2	Оценка на информационните активи и критичността им за бизнеса.	2		
Тема 2. Техники за атаки и основни източници на атаки срещу киберсигурността		**6**	**6**	
2.1	Основни типове атаки	3	3	
2.2	Смесени техники за атаки	3	3	
Тема 3. Системна сигурност		**4**	**4**	
3.1	Подобряване на сигурността на Windows и Linux системи.	2	2	
3.2	Откриване и предотвратяване от проникване в системата.	2	2	
3.3	Конфигуриране и мониторинг на сървъри и хостове.			
Тема 4. Уеб сигурност		**6**	**6**	
4.1	Сигурност на уеб приложенията	2	2	
4.2	Сигурност на уеб сървърите	2	2	
4.3	Криптография. Симетрично и асиметрично криптиране.	2	2	
Тема 5. Концепции за сигурност, приложени към ИКТ кибер инфраструктура		**4**	**8**	
5.1	Основни елементи на ИКТ инфраструктурата, касаещи киберсигурността	1	2	
5.2	Типични уязвимости, експлойти и заплахи в компютърните мрежи и системи	1	2	

5.3	Проверки за проникванията. Инструменти.	1	2	
5.4	Управление на уязвимостите и сканиране	1	2	
Тема 6. Кибер защита и техники за анализ		**6**	**4**	
6.1	Защита на уеб трафик. Защита със защитни стени.	2	2	
6.2	Защита на мрежови комуникации. Защита на безжични мрежи.	2	2	
6.3	Методи за проактивна защита	1		
6.4	Конфигуриране на виртуални частни мрежи	1		
	Общо:	**30**	**30**	

III. ФОРМИ НА КОНТРОЛ:

No. по ред	**ВИД И ФОРМА НА КОНТРОЛА**	**Брой**	**ИАЗ ч.**
1.	**Семестриален (текущ) контрол**		
1.1.	Практическо контролно задание	1	40
1.2.	Курсов проект	1	50
	Общо за семестриален контрол:	**2**	**90**
2.	**Сесиен (краен) контрол**		
2.1.	Изпит (тест)	1	60
	Общо за сесиен контрол:	**1**	**60**
	Общо за всички форми на контрол:	**3**	**150**

IV. ЛИТЕРАТУРА

ЗАДЪЛЖИТЕЛНА (ОСНОВНА) ЛИТЕРАТУРА:

1. Каракънева, Ю. Киберсигурност – основни аспекти. Авангард Прима, 2013.
2. Гудман, М. Киберпрестъпления. Милениум, 2016.
3. Sutton, D. Cyber Security A practitioner's guide, BCS. The Chartered Institute for IT, 2017.
4. Johnson, T.A. Cybersecurity Protecting Critical Infrastructures from Cyber Attack and Cyber Warfare. CRC Press, 2015.

ПРЕПОРЪЧИТЕЛНА (ДОПЪЛНИТЕЛНА) ЛИТЕРАТУРА:

1. Graham J., Howard, R., Olson, R. Cyber Security Essential. CRC Press, 2011.
2. Whitman, M.E., Mattord, H.J. Principles of Information Security. Boston: Cengage Learning, 2016.
3. Stallings, W. Cryptography and Network Security Principles and Practice. Pearson, 6th Ed. 2014.