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

Ф А К У Л Т Е Т „И Н Ф О Р М А Т И К А“

К А Т Е Д Р А „И Н Ф О Р М А Т И К А“

Приета от ФС (протокол № 35/25.01.2023 г.)

Приета от КС (протокол № 6/23.01.2023 г.)

УТВЪРЖДАВАМ:

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“- задочно обучение

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

СЕМЕСТЪР: 9 - СС и СНУ, 11 - ДНДО

ОБЩА СТУДЕНТСКА ЗАЕТОСТ: 210 ч.; в т.ч. аудиторна 30 ч.

КРЕДИТИ: 7

РАЗПРЕДЕЛЕНИЕ НА СТУДЕНТСКАТА ЗАЕТОСТ СЪГЛАСНО УЧЕБНИЯ ПЛАН

ВИД УЧЕБНИ ЗАНЯТИЯ	***ОБЩО (часове)***
АУДИТОРНА ЗАЕТОСТ: т. ч. • ЛЕКЦИИ • УПРАЖНЕНИЯ (семинарни занятия/ лабораторни упражнения) ИЗВЪНАУДИТОРНА ЗАЕТОСТ	 15 15 180

Изготвили програмата:

1. ……..
(проф. 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.

Ключовите компетентности, които придобиват студентите в процеса на обучение включват следните:

- *математическа компетентност и компетентност в областта на точните науки, технологиите и инженерството – способност за логическо мислене и създаване на такава организация по повод на различните аспекти на киберсигурността, които да подпомага нейната успешна защита.*
- *цифрова – способност за ползване на информационните и комуникационни технологии в контекста на управлението и защитата на различни информационни ресурси и киберсигурността.*
- *предприемаческа – способност за планиране, разработване и реализиране на проекти в областта на системната и уеб сигурността с цел постигане на надеждна кибер защита.*

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		**2**	**1**	
1.1	Ключова терминология в киберсигурността. Значение на киберсигурността.	1	1	
1.2	Оценка на информационните активи и критичността им за бизнеса.	1		
Тема 2. Техники за атаки и основни източници на атаки срещу киберсигурността		**2**	**3**	
2.1	Основни типове атаки	1	2	
2.2	Смесени техники за атаки	1	1	
Тема 3. Системна сигурност		**2**	**2**	
3.1	Подобряване на сигурността на Windows и Linux системи.	1	1	
3.2	Откриване и предотвратяване от проникване в системата.	1	1	
3.3	Конфигуриране и мониторинг на сървъри и хостове.			

Тема 4. Уеб сигурност		**3**	**3**	
4.1	Сигурност на уеб приложенията	1	1	
4.2	Сигурност на уеб сървърите	1	1	
4.3	Криптография. Симетрично и асиметрично криптиране.	1	1	
Тема 5. Концепции за сигурност, приложени към ИКТ кибер инфраструктура		**3**	**3**	
5.1	Основни елементи на ИКТ инфраструктурата, касаещи киберсигурността	1	1	
5.2	Типични уязвимости, експлойти и заплахи в компютърните мрежи и системи. Проверки за проникване. Инструменти.	1	2	
5.3	Управление на уязвимостите и сканиране	1		
Тема 6. Кибер защита и техники за анализ		**3**	**3**	
6.1	Защита на уеб трафик. Защита със защитни стени.	1	1	
6.2	Защита на мрежови комуникации. Защита на безжични мрежи.	1	1	
6.3	Конфигуриране на виртуални частни мрежи	1	1	
	Общо:	**15**	**15**	

III. ФОРМИ НА КОНТРОЛ

No. по ред	**ВИД И ФОРМА НА КОНТРОЛА[1]**	**Брой**	**ИАЗ ч.**
1.	**Семестриално оценяване**		
1.1.	Практическо контролно задание	1	40
1.2.	Разработване на курсова работа	1	50
1.3.	Защита на курсовата работа и демонстрация	1	20
	Общо за семестриалното оценяване:	**3**	**110**
2.	**Сесийно оценяване**		
2.1.	Изпит	1	70
	Общо за сесийното оценяване:	**1**	**70**
	Общо за всички форми на контрол:	**4**	**180**

IV. ЛИТЕРАТУРА

ЗАДЪЛЖИТЕЛНА (ОСНОВНА) ЛИТЕРАТУРА:

1. Каракънева, Ю. Киберсигурност – основни аспекти. Авангард Прима, 2013.
2. Гудман, М. Киберпрестъпления. Милениум, 2016.
3. Diogenes, Y., Ozkaya, E. Cybersecurity – Attack and Defense Strategies: Improve your security posture to mitigate risks and prevent attackers from infiltrating your system, Packt Publishing, 3rd Ed., 2022.
4. Wittkop, Y. The Cybersecurity Playbook for Modern Enterprises: An end-to-end guide to preventing data breaches and cyber attacks, Packt Publishing, 2022.

[1] При дисциплини, които завършват с текуща оценка се попълва само т. 1 Семестриално оценяване, съгласно чл.21, ал. 2 от Правилника за оценяване на знанията, уменията и компетентностите на студентите в Икономически университет – Варна.

ПРЕПОРЪЧИТЕЛНА (ДОПЪЛНИТЕЛНА) ЛИТЕРАТУРА:

1. Steven, M. Cyber Security: Ultimate Beginners Guide to Learn the Basics and Effective Methods of Cyber Security (An Essential Guide to Ethical Hacking for Beginners, 2019.
2. Möller, D.P.F. Cybersecurity in Digital Tranfformation-Scope and Application, Springer, 2021.