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 № 9/24.04.2024 г.)

Приета от КС (протокол № 10/16.04.2024 г.)

УТВЪРЖДАВАМ:

Декан:

(проф. д-р Владимир Сълов)

У Ч Е Б Н А П Р О Г Р А М А

ПО ДИСЦИПЛИНАТА: „УПРАВЛЕНИЕ НА ИНФОРМАЦИОННАТА СИГУРНОСТ“

ЗА СПЕЦ: „Информатика и компютърни науки“;

ОКС „бакалавър“ – редовно обучение

КУРС НА ОБУЧЕНИЕ: 4; СЕМЕСТЪР: 7

ОБЩА СТУДЕНТСКА ЗАЕТОСТ: 180 ч.; в т.ч. аудиторна 60 ч.

КРЕДИТИ: 6

РАЗПРЕДЕЛЕНИЕ НА СТУДЕНТСКАТА ЗАЕТОСТ СЪГЛАСНО УЧЕБНИЯ ПЛАН

ВИД УЧЕБНИ ЗАНЯТИЯ	***ОБЩО (часове)***	***СЕДМИЧНА НАТОВАРЕНОСТ (часове)***
АУДИТОРНА ЗАЕТОСТ: т.ч. • ЛЕКЦИИ • УПРАЖНЕНИЯ (семинарни занятия/ лабораторни упражнения)	 30 30	 2 2
ИЗВЪНАУДИТОРНА ЗАЕТОСТ	120	-

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

Целта на дисциплината „Управление на информационната сигурност" е да предложи знанията, които ще бъдат необходими на студентите, бъдещи специалисти по информационна сигурност. Тези знания са необходими и за студентите, които работят в ИТ отделите на фирми, където е необходимо да притежават съответните компетенции в областта на информационната сигурност.

Съгласно препоръката на Съвета на Европейския съюз от 22 май 2018 г. в хода на обучението по дисциплината се прилагат и развиват следните ключови компетентности:

• математическа компетентност и компетентност в областта на точните науки, технологиите и инженерството. Това включва развиване на аналитични умения и способност за прилагане на математически модели за анализ на рискове и оценка на сигурността на информационните системи.

• цифрова компетентност. Студентите ще развият умения за анализ и разбиране на компютърни системи и мрежи, включително разбиране на криптографски алгоритми, защита на данните и обработка на информацията в сигурна среда.

• личностна компетентност. Развиване на способност за ефективно комуникиране и работа в екип при решаване на проблеми в областта на информационната сигурност, както и развитие на етичния кодекс и отговорност в сферата на управлението на информационната сигурност.

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. СЪЩНОСТ НА ИНФОРМАЦИОННАТА СИГУРНОСТ. ВИДОВЕ ИНФОРМАЦИОННА СИГУРНОСТ		**4**	**3**	
1.1	Същност на информационната сигурност. Основни понятия, цели, заплахи, уязвимости	2		
1.2	Видове информационна сигурност	2		
ТЕМА 2. СИСТЕМНА СИГУРНОСТ		**3**	**6**	
2.1	Сигурност на хардуера	1		
2.2	Сигурност на операционната система	1	4	
2.3	Сигурност на приложенията	1	2	
ТЕМА 3. ОРГАНИЗАЦИОННА СИГУРНОСТ		**4**	**2**	
3.1	Рамка на информационната сигурност	2		
3.2	Политики за сигурност, стандарти, процедури и ръководства	1	2	
3.3	Одитиране на информационната сигурност	1		
ТЕМА 4. МРЕЖОВА СИГУРНОСТ		**4**	**4**	
4.1	Проектиране на сигурна мрежова инфраструктура. Мрежови протоколи и портове.	2	2	
4.2	Инструменти за мрежова сигурност – защитни стени, VPN, IDS и филтри. Сигурност на отдалечения достъп. Безжична сигурност	2	2	
ТЕМА 5. ОСНОВНИ ЗАПЛАХИ ЗА СИГУРНОСТТА НА ИНФОРМАЦИОННИТЕ СИСТЕМИ		**4**	**4**	
5.1	Вектори на заплахите. Източници, заплахи и цели на заплахите. Външни и вътрешни заплахи	1	1	
5.2	Типове атаки. Атаки със зловреден код. Видове зловреден код.	2	2	
5.3	Атаки на мрежово ниво. Атаки на ниво приложения. Други атаки	1	1	

ТЕМА 6. СИГУРНОСТ НА ДОСТЪПА ДО ИНФОРМАЦИОННИТЕ РЕСУРСИ		**4**	**4**	
6.1	Контрол на достъпа. Автентикационни модели.	3	2	
6.2	Логически и физически контрол на достъпа. Правила за имена и пароли, политики.	1	2	
ТЕМА 7. СОЦИАЛЕН ИНЖЕНЕРИНГ		**3**	**3**	
7.1	Същност на социалния инженеринг. Потенциални пробиви в сигурността в резултат на социалния инженеринг	1		
7.2	Методи, използвани в социалния инженеринг	1	2	
7.3	Политики и процедури за защита от социален инженеринг	1	1	
ТЕМА 8. УПРАВЛЕНИЕ НА СИГУРНОСТТА ЧРЕЗ ПОЛИТИКИ		**4**	**4**	
8.1	Администриране на сигурността чрез политики за потребители и компютри. Директорийна услуга	2	4	
8.2	Прилагане на политики за сигурност. Изключения от правилата за политики.	2		
	Общо:	**30**	**30**	

III. ФОРМИ НА КОНТРОЛ

No. по ред	**ВИД И ФОРМА НА КОНТРОЛА[1]**	**Брой**	**ИАЗ ч.**
1.	**Семестриално оценяване**		
1.1.	Тест с практическа насоченост	1	20
1.2.	Разработване на курсова работа	1	10
1.3.	Защита на курсовата работа	1	20
	Общо за семестриално оценяване:	**3**	**50**
2.	**Сесийно оценяване**		
2.1.	Изпит (тест)	1	70
	Общо за сесийно оценяване:	**1**	**70**
	Общо за всички форми на контрол:	**4**	**120**

IV. ЛИТЕРАТУРА

ЗАДЪЛЖИТЕЛНА (ОСНОВНА) ЛИТЕРАТУРА:

1. Димов, П., Здравков, З., Добрева, Х. Информационна сигурност. София: Военна академия „Г. С. Раковски“, 2021.
2. Death, D. Information Security Handbook: Enhance your proficiency in information security program development. Packt Publishing, 2nd Ed., 2023.

ПРЕПОРЪЧИТЕЛНА (ДОПЪЛНИТЕЛНА) ЛИТЕРАТУРА:

1. Kim D., Solomon M.G. Fundamentals of Information Systems Security. Jones & Bartlett Learning, 4th Ed., 2021.
2. Whitman, M. E. and Mattord, H. J. Principles of Information Security. Cengage, 7th Ed. 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.