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 № 27/ 26.04.2022 г.)

Приета от КС (протокол № 10/ 12.04.2022 г.)

УТВЪРЖДАВАМ:

Декан:

(проф. д-р Владимир Сълов)

У Ч Е Б Н А П Р О Г Р А М А

ПО ДИСЦИПЛИНАТА: „КРИПТИРАНЕ И ЗАЩИТА НА ДАННИ”

ЗА СПЕЦ: „Data science“; ОКС „бакалавър“ – редовно обучение

КУРС НА ОБУЧЕНИЕ: 4; СЕМЕСТЪР: 8

ОБЩА СТУДЕНТСКА ЗАЕТОСТ: 150 ч.; в т.ч. аудиторна 60 ч.

КРЕДИТИ: 5

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	90	-

Изготвили програмата:

1. ……..
(проф. д.н. Борислав Стоянов)

2. ……
(ст. преп. Цветелина Иванова)

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

I. А Н О Т А Ц И Я

Дисциплината „Криптиране и защита на данни“ е избираема за студентите от бакалавърската програма „Data science“. Тя има за цел да формира знания за алгоритмите за криптиране на данни. Получените знания са в контекста на методите за криптиране с акцент върху класическите и съвременните технологии за защита на данни. Подбраното учебно съдържание е насочен към изграждане на цифрова и личностна компетентност чрез решаването на конкретни задачи и поемане на лична отговорност за получаване на качествено образование. Компетентностите в областта на математическите и точните науки ще се изградят чрез изучаване на различни криптографски алгоритми, които стъпват върху строга математическа основа.

Развиват се следните ключови компетентности:

• Математическа компетентност и компетентност в областта на точните науки, технологиите и инженерството – група 3: Работа с масиви от данни

• Цифрова – група 4: Работа с алгоритми.

• Личностна – група 5. Умения за работа в екип, самоконтрол, упоритост, умение за общуване и комуникативност.

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**
1.	**КРИПТИРАНЕ И ЗАЩИТА НА ДАННИТЕ**	**3**	**-**	
1.1.	Криптография и криптоанализ.	1	-	
1.2.	Криптографска система	2	-	
2.	**КЛАСИЧЕСКИ СИМЕТРИЧНИ КРИПТОГРАФСКИ АЛГОРИТМИ**	**6**	**8**	
2.1.	Заместващи криптографски алгоритми	3	4	
2.2.	Разместващи криптографски алгоритми	3	4	
3.	**БЛОКОВИ КРИПТОГРАФСКИ АЛГОРИТМИ**	**7**	**7**	
3.1.	Същност и приложение	3	-	
3.2.	Блокови криптографски алгоритми	4	**7**	
4.	**ПОТОЧНИ ШИФРИ**	**7**	**8**	
4.1.	Псевдослучайни генератори	3	4	
4.2.	Преместващи регистри	4	4	
5.	**НЕСИМЕТРИЧНИ КРИПТОГРАФСКИ АЛГОРИТМИ (С ПУБЛИЧЕН КЛЮЧ)**	**7**	**7**	
5.1.	Същност и приложение	2	-	
5.2.	Несиметрични криптографски алгоритми	5	7	
	Общо:	**30**	**30**	

III. ФОРМИ НА КОНТРОЛ

No. по ред	ВИД И ФОРМА НА КОНТРОЛА[1]	Брой	ИАЗ ч.
1.	**Семестриално оценяване**		
1.1.	Курсова работа	1	20
1.2.	Контролна работа	2	30
	Общо за семестриалното оценяване:	**3**	**50**
2.	**Сесийно оценяване**		
2.1.	Изпит (тест или курсова задача)	1	40
	Общо за сесийното оценяване:	**1**	**40**
	Общо за всички форми на контрол:	**4**	**90**

IV. ЛИТЕРАТУРА

ЗАДЪЛЖИТЕЛНА (ОСНОВНА) ЛИТЕРАТУРА:

1. Електронни материали, качени в платформата за е-обучение
2. Smart, N. (2016) Cryptography, An Introduction : Third Edition, https://homes.esat.kuleuven.be/~nsmart/Crypto_Book/.

ПРЕПОРЪЧИТЕЛНА (ДОПЪЛНИТЕЛНА) ЛИТЕРАТУРА:

1. Манев, Н. (2016) Криптография, https://store.fmi.uni-sofia.bg/fmi/algebra/lect_notes_manev/NumbTh6.pdf.

[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.