ИКОНОМИЧЕСКИ УНИВЕРСИТЕТ–В А Р Н А

Ф А К У Л Т Е Т „УПРАВЛЕНИЕ“

КАТЕДРА „МЕЖДУНАРОДНИ ИКОНОМИЧЕСКИ ОТНОШЕНИЯ“

Приета от ФС (протокол № 12/ 29.04.2024)
Приета от КС (протокол № 8/ 16.04.2024)

УТВЪРЖДАВАМ:
Декан:
(доц. д-р Добрин Добрев)

У Ч Е Б Н А П Р О Г Р А М А

ПО ДИСЦИПЛИНАТА: „КИБЕРСИГУРНОСТ И КИБЕР УСТОЙЧИВОСТ ”

ЗА СПЕЦ: „Международни икономически отношения“; 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. **……..**
   (гл. ас. д-р М. Камджалов)
2. **……**
   (доц. д-р Г. Маринов)

Ръководител катедра: ……..
„ Международни икономически отношения “
(проф. д-р В. Димитрова)

I. А Н О Т А Ц И Я

Курсът "Киберсигурност и кибер устойчивост" има за цел да предостави знания за съвременните заплахи в киберпространството и начините за защита на кибер активите. Студентите ще бъдат научени да оценяват заплахите за киберсигурността, като използват различни аналитични техники и методологии. Курсът акцентира върху оценката на риска, откриването на кибер уязвимости, прилагането на техники за смекчаване на кибер заплахите и развитието на умения за кибер устойчивост за корпоративни цели.

Ключови компетентности, развити по време на курса: цифрови и граждански.

II. ТЕМАТИЧНО СЪДЪРЖАНИЕ

No. по ред	НАИМЕНОВАНИЕ НА ТЕМИТЕ И ПОДТЕМИТЕ	БРОЙ ЧАСОВЕ		
		Л	СЗ	ЛУ
1.	**Основи на киберсигурността**	**2**	**2**	
1.1	Произход			
1.2	Мрежова сигурност			
1.3	Рискове за киберсигурността			
2.	**Концепции за компютърна сигурност**	**2**	**2**	
2.1	Определение за компютърна сигурност			
2.2	Предизвикателствата на компютърната сигурност			
2.3	Примери			
3.	**Криптографията като фундамент на киберсигурността**	**2**	**2**	
3.1	Криптографията като уравнение			
3.2	Интегритет и хашинг			
3.3	Криптография и невъзможност за отхвърляне			
4.	**Киберсигурност и управление на риска**	**2**	**2**	
4.1	Идентификация на заплахи			
4.2	Стъпки за намаляване на кибер рисковете			
5.	**Приложения за киберсигурност**	**2**	**2**	
5.1	Потребителско име и парола			
5.2	VPN мрежи			
5.3	Блокчейн технология			
6.	**Морска киберсигурност**	**2**	**2**	
6.1	Характеристики			
6.2	Роли, отговорности и задачи			
7.	**Пристанищна киберсигурност**	**2**	**2**	
7.1	Пристанищни власти			
7.2	Проблеми с киберсигурността на пристанищните структури			
8.	**Социално инженерство**	**2**	**2**	
8.1	Същност			
8.2	Социално инженерство и киберсигурност			
8.3	Защита срещу социално инженерство			
9.	**Основни концепции за кибернетична устойчивост**	**2**	**2**	
9.1	Необходимостта от киберустойчивост			

9.2	Устойчивост и системи			
9.3	Оценка			
10. Кибер зависимости		**2**	**2**	
10.1	Дефиниране			
10.2	Идентифициране на кибер зависимости			
10.3	Управление на риска от кибер зависимости			
11. Моделиране на въздействието на кибератаките		**2**	**2**	
11.1	Техники			
11.2	Архитектура и изпълнение			
11.3	Казуси			
12. Подобряване на кибер устойчивостта		**2**	**2**	
12.1	Техники за активна защита			
12.2	Управление на човешкия фактор			
12.3	Намаляване на вътрешните заплахи			
13. Интернет на нещата		**2**	**2**	
13.1	Кибер-физически системи от следващо поколение			
13.2	Устойчивост в контекста на интелигентните градове			
14. Вериги за доставки		**2**	**2**	
14.1	Преглед на веригата за доставки на електроника			
14.2	От риск към устойчивост в глобалните вериги за доставки			
14.3	Примери			
15. Икономическа ефективност		**2**	**2**	
15.1	Основни принципи			
15.2	Разходи за кибер прекъсвания			
15.3	Смекчаване на кибер прекъсванията			
	Общо:	**30**	**30**	

III. ФОРМИ НА КОНТРОЛ

No. по ред	ВИД И ФОРМА НА КОНТРОЛА[1]	Брой	ИАЗ ч.

[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.

1.	**Семестриално оценяване**		
1.1.	Курсов проект	**1**	**30**
1.2.	Тест	**2**	**30**
	Общо за семестриалното оценяване:	**3**	**60**
2.	**Сесийно оценяване**		
2.1.	Изпит	**1**	**60**
	Общо за сесийното оценяване:	**1**	**60**
	Общо за всички форми на контрол:	**4**	**120**

IV. ЛИТЕРАТУРА

ЗАДЪЛЖИТЕЛНА (ОСНОВНА) ЛИТЕРАТУРА:

1. Wilson, D. *Cybersecurity*. The Massachusetts Institute of Technology Press, 2021.
2. Kott, A. and Linkov, I. *Cyber Resilience of Systems and Networks*, Springer International Publishing AG, 2019. https://doi.org/10.1007/978-3-319-77492-3

ПРЕПОРЪЧИТЕЛНА (ДОПЪЛНИТЕЛНА) ЛИТЕРАТУРА:

1. Conti, M. Somani, G. and Poovendran, R. *Versatile Cybersecurity*, Springer Nature Switzerland AG, 2018. https://doi.org/10.1007/978-3-319-97643-3
2. Eric C. *Cybersecurity Incident Response: How to Contain, Eradicate, and Recover from Incidents*, Thompson Lisle, Illinois, USA, 2018.
3. *The Cyber Resilience Index: Advancing Organizational Cyber Resilience*, World Economic Forum, 2022.
4. *The Guidelines on Cyber Security Onboard Ships,* issued by ICS, IUMI, BIMCO, OCIMF, INTERTANKO, INTERCARGO, InterManager, WSC and SYBAss.