MD-2004, CHIŞINĂU, STR. ŞTEFAN CEL MARE 168, TEL: 022 23-54-41 | www.utm.md

G.O.001 ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И КИБЕРБЕЗОПАСНОСТЬ

1. Данные о дисциплине/модуле

Факультет	Электроника и телекоммуникации				
Отделение	Телекоммуникации и электронные системы				
Цикл обучения	Степень бакалавра, первый цикл				
Программы обучения	0714.1 ТЕХНОЛОГИИ И ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ В СЕТЯХ ЭЛЕКТРОННОЙ СВЯЗИ 0710.1 ИНЖЕНЕРИЯ И МЕНЕДЖМЕНТ В ЭЛЕКТРОННЫХ КОММУНИКАЦИЯХ 0714.6 БЕЗОПАСНОСТЬ ЭЛЕКТРОННЫХ КОММУНИКАЦИЙ				
Год обучения	**семестр**	**Тип оценки**	**Формирующая категория**	**Категория факультативности**	**Кредит ECTS**
I - очной формы обучения II - заочной формы обучения	I III	E	G – Учебные модули/блоки для формирования общих навыков и компетенций	O – обязательный учебный блок	3

2. Расчетное общее время

Общее количество часов в учебной программе	Из которого				
	Часы работы аудитории		Индивидуальная работа		
	Курс	Практикум	Проект года	Изучение теоретического материала	Подготовка заявления
90	30	15	-	30	15
90	10	8	-	36	36

3. Предварительные условия для доступа к дисциплине/модулю

Согласно учебному плану	Информатика, Математика, Физика
Согласно компетенциям	Общие знания о структуре информационных систем, аппаратных компонентах, операционных системах.

4. Условия осуществления образовательного процесса для

Курс	Для представления теоретического материала в аудитории требуется доска, проектор и компьютер. Опоздания студентов, а также телефонные разговоры во время лекции не будут допущены. В случае онлайн-занятий они будут проводиться через Microsoft Teams.
лабораторная работа/ семинар	Студенты будут выполнять лабораторные работы в соответствии с методическими указаниями. Они подготовят отчеты в электронном формате, которые загрузят на платформу Moodle не позднее недели после выполнения работы.

5. Приобретенные специальные навыки

Общие навыки, которые необходимо развивать	**Для образовательной программы IMCE необходимо развить следующие общие и профессиональные компетенции:** CG1. Использование в профессиональной деятельности базового законодательства, определенного в фундаментальных науках. CG 1.1. Применять базовые принципы и соответствующие правовые нормы для использования информации и кибербезопасности. CG 1.2. Соблюдать этические и правовые нормы, касающиеся защиты данных и интеллектуальной собственности в цифровой среде. CG2. Применение результатов маркетинговых исследований при разработке конкурентоспособных продуктов/услуг. CG 2.1. Анализировать потребности рынка в ИТ-продуктах и услугах по кибербезопасности. CG 2.2. Предлагать инновационные ИТ-решения и услуги на основе анализа рынка и маркетинговых исследований. **Для учебных программ SCE и TSRC необходимо развивать следующие общие и профессиональные компетенции:**

	CG2. Применение результатов маркетинговых исследований при разработке конкурентоспособных продуктов/услуг. CG 2.1. Анализ потребностей рынка в ИТ-продуктах и услугах по кибербезопасности. CG 2.2. Предложение инновационных ИТ-решений и услуг на основе анализа рынка и маркетинговых исследований. CG4. Обеспечение соблюдения нормативно-правовой базы в области охраны труда и окружающей среды. CG4.1. Применение правил техники безопасности и гигиены труда, оценка профессиональных рисков на рабочем месте. CP1. Идентификация технологий, используемых в области электронных коммуникаций. CP1.1. Определение характеристик технологий, используемых в области электронных коммуникаций при проектировании и эксплуатации сетей связи.
Профессиональные навыки, которые необходимо развивать	**Для образовательной программы IMCE необходимо развить следующие общие и профессиональные компетенции:** CP4. Использование специализированных языков программирования. CP 4.1. Писать, тестировать и отлаживать код с использованием специализированных языков программирования для разработки безопасных приложений. CP 4.2. Внедрять алгоритмы и структуры данных для решения конкретных задач по информационной безопасности. CP 4.3. Использовать среды разработки и специализированные инструменты для создания программного обеспечения. **Для учебных программ SCE и TSRC необходимо развивать следующие общие и профессиональные компетенции:** CP1. Идентификация технологий, используемых в области электронных коммуникаций. CP1.1. Определение характеристик технологий, используемых в области электронных коммуникаций при проектировании и эксплуатации сетей связи.

6. Цели курса/модуля

Общая цель	Знание компонентов аппаратного обеспечения, операционных систем. Реализация процесса установки, настройки и устранения неполадок информационных систем.
Конкретные цели	Знание специфических понятий информационных технологий. Установка и использование различных аппаратных и программных компонентов. Оптимальная настройка программного обеспечения. Устранение проблем с аппаратным обеспечением и операционными системами. Знание общих проблем и решений, связанных с аппаратными компонентами и операционными системами.

7. Содержание курса/модуля

Тематика учебной деятельности	**очное обучение**	**заочное обучение**
T1. Введение в компьютерные сети.	2	0,5
T2. Сетевые модели и протоколы.	2	0,5
T3. Физический уровень.	2	1
T4. Системы счисления.	2	1
T5. Сеть Ethernet.	2	1
T6. Сетевой уровень.	2	1
T7. Транспортный и прикладной уровни.	2	0,5
T8. Основные понятия в области кибербезопасности.	2	0,5
T9. Техники и типы кибератак.	2	0,5
T10. Защита данных и конфиденциальности в интернете.	2	0,5
T11. Стратегии защиты сетей, оборудования и данных.	2	1
T12. Современное программирование с Web 2.0 и Web 3.0.	2	1
T13. Облачные технологии.	2	0,5
T14. Искусственный интеллект и машинное обучение (Machine Learning).	2	0,5
T15. Автоматизация и её роль в области кибербезопасности.	2	
Всего лекций:	**30**	**10**

LL1. Packet Tracer. Моделирование сетей.	1	0,5
LL2. Изучение физического уровня.	2	1
LL3. IP-адресация.	2	0,5
LL4. Обмен данными через протоколы TCP и UDP.	2	0,5
LL5. Поиск работы в сфере кибербезопасности.	1	1
LL6. Исследование шифрования файлов и данных. Проверка целостности файлов и данных.	1	1
LL7. Обнаружение уязвимостей и угроз.	1	1

LL8. Использова-ние стеганографии	1	0,5
LL9. Настройка транспортного модуля VPN.	2	1
LL10. Настройка туннельного модуля VPN.	2	1
Всего лабораторных работ:	**15**	**8**

8. Библиографические ссылки

Обязательные	1. Hotărârea Parlamentului Nr. HP391/2023 din 15.12.2023 privind aprobarea Strategiei securității naționale a Republicii Moldova, publicat: 17.01.2024 în MONITORUL OFICIAL Nr. 17-19, https://presedinte.md/app/webroot/uploaded/Proiect%20SSN_2023.pdf 2. Ludmila PECA, Dinu ȚURCANU. Network security: Practical examples solved to be introduced in network security. SBN 978-9975-45-941-9. Chișinău, Publisher „Tehnica-UTM", 2023. Disponibil: http://repository.utm.md/bitstream/handle/5014/22819/Network-security-Practical-examples-Guide.pdf?sequence=1&isAllowed=y 3. Cisco Networking Academy. Introducere în Securitatea Cibernetică - este un curs care oferă informații despre securitatea online, diferitele tipuri de malware și atacuri cibernetice, măsurile luate de companii pentru a le elimina / Cisco Systems, 2022, https://www.netacad.com/portal/web/self-enroll/m/course-1226327 4. Cisco Networking Academy. Curs CCNA Routing & Switching / Cisco Systems, 2023, https://www.netacad.com/ 5. https://paloaltonetworksacademy.net/course/view.php?id=2351 6. https://paloaltonetworksacademy.net/course/view.php?id=2355
Дополнительные	1. Hotărârea Guvernului Nr. 811 din 29-11-2015 cu privire la Programul național de securitate cibernetică a Republicii Moldova pentru anii 2016-2020. Ministerul Justiției, https://www.legis.md/cautare/getResults?doc_id=110324&lang=ro 2. Ludmila PECA, Dinu ȚURCANU. Computer networks: Practical examples solved to be introduced in computer networks. ISBN 978-9975-45-812-2. Chișinău, Publisher „Tehnica-UTM", 2022. http://repository.utm.md/bitstream/handle/5014/20549/Computer-networks-Practical-examples-DS.pdf?sequence=1&isAllowed= 3. Ghid de bune practici privind asigurarea securității pe rețelele sociale, I.P. Serviciul Tehnologia Informației și Securitate Cibernetică, https://stisc.gov.md/sites/default/files/ghiduri/Ghid%20de%20bune%20practici.pdf 4. Ghid de bune practici pentru securitate cibernetică, Serviciul Român de Informații, https://www.sri.ro/assets/files/publicatii/ghid_de_securitate_cibernetica.pdf 5. Iulian ALECU, Costel CIUCHI, Toma CÎMPEANU, Iulian COMAN, Larisa GĂBUDEANU, Ioan-Cosmin MIHAI, Cosmina MOGHIOR, Nelu MUNTEANU, Gabriel PETRICĂ, Ionuț STOICA, Cătălin ZETU. Ghid de securitate cibernetică, 2021, ISBN: 978-973-0-33645-0, DOI: 10.19107/CYBERSEC.2021.RO, https://dnsc.ro/vezi/document/ghid-securitate-cibernetica-2021

9. Оценка

Периодический		Транслировать	Индивидуальное обучение	Проект/диссертация	Экзамен
ЭП 1	ЭП 2				
15%	15%	15%	15%	-	40%
Минимальный стандарт успеваемости : Посещение и активность на лекциях и лабораторных работах; Получение минимальной оценки «5» по обеим аттестациям , учитывающим активность студента на лекциях и лабораторных работах ; Получение минимальной оценки «5» в технических характеристикахПолучение минимальной оценки «5» на итоговом экзамене .					