MD-2004, Chișinău, bd. Ștefan cel Mare, 168, TEL. 022-23-54-58 | www.utm.md/

D.05.O.038 SECURITATEA INFORMAȚIONALĂ

1. Данные о дисциплине

Факультет	Факультет электроники и телекоммуникаций				
Департамент	Телекоммуникации и электронные системы				
Цикл обучения	Цикл I – бакалавриат, высшее образование				
Образовательная программа	**0714.2 ТЕЛЕКОММУНИКАЦИОННЫЕ СЕТИ И ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ**				
Год обучения	Семестр	Тип оценки	Образовательная категория	Категория опциональности	Кредиты ECTS
III (очная форма обучения); IV (заочная форма обучения).	5 7	E	D - Профессиональная учебная единица	O – *Обязательная* учебная единица	6

2. Общее расчетное время

Общее количество часов в учебном плане	Из которых				
	Часы в аудитории		Часы в аудитории		
	Лекции	Лабораторные/ Практическая работа	Proiect de an	Изучение теоретического материала	Выполнение практических заданий
180	45	30/15	-	45	45
180	16	12/8	-	72	72

3. Предпосылки для доступа к дисциплине

Согласно учебному плану	Для изучения Информационной Безопасности необходима solidная база в математике (криптография), компьютерных сетях и операционных системах. Также знания программирования являются важными.
В соответствии с компетенциями	По завершении курса вы сможете защищать данные и системы от кибератак. Вы научитесь оценивать риски, внедрять меры безопасности (такие как шифрование и фаерволы) и реагировать на инциденты. Курс охватывает как методы наступательной безопасности (тестирование на проникновение), так и защитной.

4. Условия проведения образовательного процесса для:

Лекции	Для представления материала в аудитории необходимы интерактивная доска, проектор и компьютер. Не будут допускаться опоздания студентов, а также телефонные разговоры во время занятий.
Практических работ	Студенты будут ориентированы на текущую подготовку к каждому занятию практических работ (изучение конспектов лекций, учебников и специализированных библиографических источников), решение примеров и задач для усвоения материала, подготовку рефератов и тематических докладов и т.д.

5. Накопленные специфические компетенции

Профессиональные компетенции	С4. Эффективная организация деятельности и эксплуатация мультимедийных услуг, основанная на понимании и применении фундаментальных понятий в области коммуникаций и передачи информации, а также на разработке и внедрении методов оценки экономической эффективности развития сферы электронных коммуникаций. С4.1. Идентификация фундаментальных концепций, касающихся передачи информации и аналоговых и цифровых коммуникаций. С4.2. Объяснение и интерпретация основных требований и специфических подходов к передаче данных, голоса, видео и мультимедиа. С.4.3. Решение практических задач с использованием общих знаний о мультимедийных

	технологиях. С.4.4. Использование основных специфических параметров в оценках, основанных на концепции качества услуг в коммуникациях. С.4.5. Организация и мониторинг деятельности экономических субъектов в соответствии с нормативной базой и требованиями деловой среды. С4.6. Развитие продуктивных отношений сотрудничества в командах; применение и рационализация инструментов мотивации их участников. С5. Интеграция, эксплуатация и управление электронными коммуникациями в различных областях национальной экономики. С5.1. Определение принципов, лежащих в основе основных технологий телекоммуникаций, стационарных и мобильных, через различные среды передачи. С5.2. Объяснение и интерпретация фундаментальных технологий и протоколов для интегрированных стационарных и мобильных систем связи. С.5.3. Установка, настройка и эксплуатация сетей связи. С.5.4. Использование методов оценки и диагностики систем и оборудования связи. С.5.5. Обеспечение средствами связи объекта небольшой/средней сложности. С.5.6. Применение управленческих инструментов для оценки эффективности и результативности деятельности, для оптимизации и мобилизации резервов и мер по повышению эффективности. С6. Использование информационных технологий, специфичных для данной области, с целью организации решения типовых задач широкополосных сетей связи и ведения бухгалтерского и финансового учёта в области электронных коммуникаций. С6.1. Идентификация / Определение / Представление законов электромагнитного поля при решении специфических задач распространения и передачи, а также специфических цепей. С6.2. Объяснение специфических методов внедрения коммуникационных технологий. С.6.3. Решение практических задач с использованием методов проектирования микроволновых цепей, планирования, охвата, выбора и размещения приемо-передающего оборудования. С.6.4. Использование основных параметров качества и методов измерения, специфичных для сред распространения и передачи. С.6.5. Разработка проектов малой/средней сложности, касающихся приемо-передающего оборудования. С.6.6. Разработка и координация проектов, относящихся к управлению бизнесом, с эффективным использованием организационных ресурсов.

6. Цели учебной единицы

Общая цель	Основная цель курса по Информационной Безопасности — предоставить тебе знания и навыки, необходимые для защиты информационных систем и данных от киберугроз. Ты научишься основным концепциям риска, уязвимости и кибератак, а также основам безопасности систем, сетей и приложений. Задача курса — подготовить тебя к планированию, внедрению и управлению эффективными решениями по безопасности в соответствии с национальными и международными стандартами.
Специфические цели	Конкретные цели курса по Информационной Безопасности структурированы таким образом, чтобы обеспечить тебе как практическое, так и теоретическое понимание области. По завершении курса ты должен будешь знать основные принципы безопасности, такие как Конфиденциальность, Целостность и Доступность (модель CIA). Ты научишься выявлять типы угроз и кибератак, от вредоносного ПО и фишинга до атак DoS и социальной инженерии.

7. Содержание учебной единицы

Тематика учебной деятельности	Количество часов	
	очная форма обучения	заочная форма обучения
Тематика лекций		
Тема 1. Киберугрозы и уязвимости – типы и характеристики.	4	1
Тема 2. Методы атак на конечные системы и техники защиты.	6	2
Тема 3. Физическая и информационная безопасность конечных устройств.	5	1
Тема 4. Принципы аутентификации и контроля доступа в сетях конечных	6	2

устройств.		
Тема 5. Программные приложения для мониторинга и обеспечения безопасности конечных устройств.	6	2
Тема 6. Механизмы шифрования и целостность данных в конечных системах.	5	1
Тема 7. Безопасность операционных систем Windows и Linux.	2	1
Тема 8. Обнаружение и защита от вредоносного ПО на конечных устройствах.	3	2
Тема 9. Внедрение решений для защиты конечных устройств: антивирус, HIDS, NIDS.	4	2
Тема 10. Оценка рисков и меры профилактики в безопасности конечных устройств.	4	2
Итого:	**45**	**16**

Тематика учебной деятельности	Количество часов	
	очная форма обучения	заочная форма обучения
Тематика практических работ		
LP1. Настройка и использование инструментов для обнаружения угроз на конечных устройствах.	2	1
LP2. Внедрение антивирусных и антивредоносных решений на конечных системах.	2	1
LP3. Настройка аутентификации и контроля доступа на конечных устройствах	2	1
LP4. Установка и настройка межсетевых экранов (firewall) для защиты конечных устройств.	2	1
LP5. Использование логов для выявления атак на конечные системы.	2	1
LP6. Применение методов шифрования для защиты данных на конечных устройствах.	2	1
LP7. Анализ и устранение уязвимостей в системах Windows/Linux.	2	1
LP8. Симуляция кибератак и применение мер защиты.	1	1
Итого:	**15**	**8**

Тематика учебной деятельности	Количество часов	
	очная форма обучения	заочная форма обучения
Тематика лабораторных работ		
LL1. Настройка и использование инструментов мониторинга безопасности конечных устройств.	4	1
LL2. Установка и настройка системы обнаружения вторжений (IDS).	4	2
LL3. Обнаружение и изоляция вредоносного ПО с использованием специализированных приложений.	4	1,5
LL4. Внедрение механизмов резервного копирования и восстановления данных конечных устройств.	8	2
LL5. Настройка протоколов безопасности для доступа к ресурсам в сетях конечных устройств.	2	1,5
LL6. Анализ сетевого трафика и выявление подозрительной активности.	2	1,5
LL7. Симуляция фишинговых атак и меры профилактики на конечных устройствах.	6	1,5
Итого:	**30**	**12**

8. Библиографические ссылки

Основные	1. CISCO Networking Academy, Endpoint Security www.netacad.com
Дополнительные	1. Leitner Achim, "Rețele WLAN sigure, cu un tunel OpenVPN criptat", Linux Magazin, nr. 22, iunie 2005; 2. Lachi A., Securitatea Sistemelor Informaționale, Partea I, Îndrumar de laborator, UTM, Chișinău, 2015;

9. Оценка

Форма обучения	Периодическая		Текущая	Индивидуальная работа	Итоговый экзамен
	Аттестация 1	Аттестация 2			
Очная	15%	15%	15%	15%	40%
Заочная	25%			25%	50%
Минимальный стандарт производительности					
Посещение и активность на лекциях и практических занятиях. Получение минимальной оценки «5» как по аттестациям, связанным с деятельностью Студента на лекциях, так и по практической работе. Получение минимальной оценки «5» на итоговом экзамене.					