СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ТЕЛЕКОМУНІКАЦІЙ

Галузь знань	12 Інформаційні технології
Шифр та назва спеціальності	125 Кібербезпека та захист інформації
Назва освітньо-професійної програми	Кібербезпека та захист інформації
Рівень вищої освіти	Перший (бакалаврський)
Факультет	Інформаційних технологій і кібербезпеки
Кафедра	Кібербезпеки та технічного захисту інформації
Статус навчальної дисципліни	ОК-17 ОПП «Кібербезпека та захист інформації»
Форма навчання	Денна

Викладач

Севастєєв Євген Олександрович
Seva.odessa@gmail.com

Старший викладач кафедри Кібербезпеки та технічного захисту інформації

Загальна інформація про дисципліну

Анотація до дисципліни	Дисципліна «Забезпечення безпеки телекомунікацій» розглядає важливі аспекти забезпечення безпеки інформації в сучасних телекомунікаційних системах. Курс розроблений з метою підготовки студентів до розуміння та впровадження стратегій та технічних методів захисту даних у мережевому середовищі. В рамках цієї дисципліни розглядаються такі питання, мережеві загрози та інциденти, методи виявлення та реагування на інциденти, контроль доступу, безпека мережевого обладнання та програмного забезпечення, а також адміністрування безпеки мережі. Окремо розглядаються технології що використовуються в корпоративних мережах, в мережах операторів та провайдерів зв'язку. Студенти отримають знання та практичні навички, необхідні для ефективного захисту інформації в мережевому середовищі, відповідно до сучасних стандартів і вимог безпеки. Після завершення курсу, вони зможуть визначати потенційні загрози, розробляти стратегії захисту і використовувати різноманітні інструменти для забезпечення конфіденційності, цілісності та доступності інформації в комп'ютерних та телеком мережах
Мета дисципліни	Основна мета навчальної дисципліни «Забезпечення безпеки телекомунікацій полягає у засвоєнні студентами знань, вмінь і навичок, що стосуються безпеки комп'ютерних мереж. Деякі можливі аспекти, які можуть бути включені у мету дисципліни, включають: розуміння загальних принципів кібербезпеки, включаючи ідентифікацію потенційних загроз та ризиків; освоєння стратегій та технік захисту мереж і даних від несанкціонованого доступу, зламу та інших загроз; ознайомлення з сучасними стандартами, протоколами та методами шифрування та аутентифікації в сучасних мережах; планування заходів безпеки та реагування на інциденти. Загальна мета полягає у тому, щоб студенти засвоїли основні принципи та практики забезпечення безпеки телекомунікацій і були готові до викликів і загроз, пов'язаних з цією галуззю.
Компетентності, формуванню яких сприяє дисципліна	КЗ 1. Здатність застосовувати знання у практичних ситуаціях. КЗ 2. Знання та розуміння предметної області та розуміння професії. КЗ 5. Здатність до пошуку, оброблення та аналізу інформації. КФ 1. Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі інформаційної та/або кібербезпеки. КФ 2. Здатність до використання інформаційнокомунікаційних технологій, сучасних методів і моделей інформаційної та/або кібербезпеки. КФ 4. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки. КФ 5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки. КФ 7. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.). КФ 9. Здатність здійснювати професійну діяльність на основі впровадження системи управління інформаційною

	та/або кібербезпекою. КФ 11. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційнотелекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки.
Результати навчання	ПРН 4. Аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач та практичних проблем у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення. ПРН 10. Виконувати аналіз та декомпозицію інформаційно-телекомунікаційних систем. ПРН 12. Розробляти моделі загроз та порушника. ПРН 13. Аналізувати проекти інформаційно-телекомунікаційних систем базуючись на стандартизованих технологіях та протоколах передачі даних. ПРН 14. Вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень. ПРН 15. Використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій. ПРН 21. Вирішувати задачі забезпечення та супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління доступом згідно встановленої політики безпеки в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах. ПРН 22. Вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно-телекомунікаційних системах згідно встановленої політики інформаційної і\або кібербезпеки. ПРН29. Здійснювати оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційно-телекомунікаційних системах та ефективності використання комплексів засобів захисту в умовах реалізації загроз різних класів. ПРН 35. Вирішувати задачі забезпечення та супроводу комплексних систем захисту інформації, а також протидії несанкціонованому доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах згідно встановленої політики інформаційної і\або кібербезпеки. ПРН 37. Вимірювати параметри небезпечних та завадових сигналів під час інструментального контролю процесів захисту інформації та визначати ефективність захисту інформації від витоку технічними каналами відповідно до вимог нормативних документів системи технічного захисту інформації. ПРН 38. Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик інформаційно-телекомунікаційних систем відповідно до вимог нормативних документів системи технічного захисту інформації. ПРН 39. Проводити атестацію (спираючись на облік та обстеження) режимних територій (зон), приміщень тощо в умовах додержання режиму секретності із фіксуванням результатів у відповідних документах.

	ПРН 40. Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик ІТС відповідно до вимог нормативних документів системи технічного захисту інформації. ПРН 46. Здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно-телекомунікаційних системах. ПРН 47. Вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації.
Обсяг дисципліни	Загальний обсяг дисципліни: 10 кредитів ЄКТС 300 годин.
Форма підсумкового контролю	Іспит
Терміни викладання дисципліни	Дисципліна викладається у 1-му та 2-му семестрі

Програма дисципліни

Модуль 1 Мережеві протоколи та технології. Атаки та захист

Тема 1.	*Поняття забезпечення безпеки телекомунікацій. основні визначення* Вступ до дисципліни. Мета та задачі захисту інформації в корпоративних комп'ютерних мережах. Основні визначення, що використовуються в сфері захисту інформації
Тема 2.	*Моделі OSI та TCP/IP з позиції безпеки* Історична ретроспектива: Зміна підходів до безпеки в телекомунікаціях
Тема 3.	*Мережеві протоколи та атаки на них* Поняття physical layer security. Протоколи канального рівня та атаки на них. Методи захисту від атак на протоколи канального рівня.
Тема 4.	*Мережеві протоколи та атаки на них ч.2* Захист інформації на мережевому та транспортному рівні. Протоколи безпеки рівня сеансу та додатків.
Тема 5.	*Конфіденційність даних в корпоративних радіомережах* Захист бездротових мереж: шифрування, ідентифікація та захист від несанкціонованого доступу
Тема 6.	*Атаки на Wi-fi мережі* Атаки на Wi-fi. Методи захисту
Тема 7.	*Телефонні мережі загального користування та їх захист* Принципи передачі голосу. Аналогова телефонія. Цифрова телефонія. Кодеки. VoIP. SIP. RSTP. Конвергентні мережі зв'язку
Тема 8.	*Технології віддаленого доступу – Remote Access.*

	Модуль 2 ***Побудова захищених корпоративних мереж***
Тема 9.	*Аналіз загроз безпеці корпоративних мереж: типові атаки та потенційні ризики*
Тема 10.	*Архітектура захищених корпоративних мереж: проектування та розгортання безпечної інфраструктури* Елементи безпечної архітектури компютерної мережі – Firewall, NAT, Proxy, Sandbox, VPN, BYOD та інші.
Тема 11.	*Фаєрвол для захисту периметру мережі в сучасних умовах* Захист мережевого периметру: перехоплення та контроль вхідного/вихідного трафіку**.** *NGFW.* Контроль додатків. Захист мережі від несанкціонованого доступу. Системи IDPS.
Тема 12.	*Захист мережевого доступу: аутентифікація, авторизація та аудит безпеки* AAA. Види аутентифікації. Логи та аудит безпеки.
Тема 13.	*Захист передачі даних: шифрування, використання віртуальних приватних мереж (VPN) та захист від перехоплення* Протоколи VPN на різних рівнях моделі OSI. PPTP, L2TP, IPSec, OpenVPN та Wireguard
Тема 14.	*Захист даних у сховищах: контроль доступу, шифрування даних та моніторинг безпеки*
Тема 15.	*Захист від вторгнень та зламу: виявлення та реагування на інциденти, моніторинг та логування подій*
Тема 16.	*Захист додатків та серверів: вразливості, патчі та механізми захисту.*
Тема 17.	*Безперервність бізнесу та відновлення після кризи: планування, відновлення та тестування резервних копій*
Тема 18.	*Захист мережі від інсайдерів*

Список рекомендованих джерел

1. Методи та засоби захисту інформації [Навчальний посібник] / В.А. Лахно, Є.В. Василіу, В.М. Гладких, В.М. Домрачев, Н.М. Сивкова. – К. : ЦП «Компринт» О.В., 2021. – 444 с.
2. Методи та засоби захисту інформації: Навчальний посібник для студентів вищих навчальних закладів./А.М. Олейніков. –Харків:НТМТ, 2014. –298с.
3. Applied Network Security by Arthur Salmon, Warun Levesque, Michael McLafferty. - Publisher: Packt Publishing, 2017.
4. CISSP All-in-One Exam Guide, Eighth Edition 8th / S. Harris, F. Maymi., 2018. – 1408 с.

Інформація про консультації

Загальна схема оцінювання

Сума балів за всі види	**Шкала**	**Оцінка за національною шкалою**	**=**	**Бали нараховуються таким чином:**

навчальної діяльності	ЄКТС	для іспиту	для заліку		
90-100	A	Відмінно	зараховано		***Оцінювання знань здобувачів вищої освіти здійснюється за 100-бальною шкалою*** і становить: за поточну успішність (участь у практичних заняттях, виконання практичних завдань та контрольних робіт) – до 60 балів, за результати екзамену – до 40 балів.
82-89	B	Добре			
74-81	C				
64-73	D	Задовільно			
60-63	E				
35-59	FX	Незадовільно з можливістю повторного складання	Не зараховано з можливістю повторного складання		
0-34	F	Незадовільно з обов'язковим повторним вивченням дисципліни	Не зараховано з обов'язковим повторним вивченням дисципліни		

Політика опанування дисципліни

Відвідування: Здобувачі вищої освіти самостійно планують відвідування лекційних занять, що проводяться в межах дисципліни. Присутність на практичних заняттях, лабораторних заняттях та контрольних заходах (екзамен/залік) є обов'язковою. При проведенні занять в онлайн режимі, присутність здобувача враховується у разі відкритого вікна.

Дотримання принципів академічної доброчесності: Підготовка усіх завдань, письмових робіт і т. ін., що виконуються в межах дисципліни, здійснюється здобувачем вищої освіти самостійно, на засадах академічної доброчесності. Викладач має право для перевірки робіт застосовувати програму **Unicheck.**

Умови зарахування пропущених занять:

Інші умови: