ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

ЗАТВЕРДЖУЮ
Декан факультету ІТ
_____ Тетяна ГОВОРУЩЕНКО
Підпис Ім'я, ПРІЗВИЩЕ
«31» 08 2024 р.

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Комплексні системи захисту інформації

Галузь знань	12 – Інформаційні технології
Спеціальність	125 – Кібербезпека
Рівень вищої освіти	Перший бакалаврський
Освітньо-професійна програма	Кібербезпека
Обсяг дисципліни	6 кредитів ЄКТС
Шифр дисципліни	ОПП.16
Мова навчання	Українська
Статус дисципліни	Обов'язкова, дисципліна професійної підготовки
Факультет	Інформаційних технологій
Кафедра	Кібербезпеки

Форма навчання	Курс	Семестр	Обсяг дисципліни		Кількість годин						Курсовий проєкт	Курсова робота	Форма семестрового контролю	
					Аудиторні заняття					Самостійна робота, у т.ч. ІРС				
			Кредити ЄКТС	Години	Разом	Лекції	Лабораторні роботи	Практичні заняття	Семінарські заняття				Залік	Іспит
Очна (денна)	4	7	6	180	68	34	34			112	+			+

Робоча програма складена на основі освітньо-професійної програми «Кібербезпека» першого (бакалаврського) рівня вищої освіти за спеціальністю 125 «Кібербезпека»

Робоча програма складена _____ Євгеній ЗАРЕЦЬКИЙ
Підпис(и) автора(ів)
канд. техн. наук, доц. Віктор ЧЕШУН
Ступінь, вчене звання, Ім'я, ПРІЗВИЩЕ автора(ів)

Схвалена на засіданні кафедри Кібербезпеки

Протокол від 30.08.2024 № 1 Зав. кафедри _____ Юрій КЛЬОЦ
Підпис Ім'я, ПРІЗВИЩЕ

Робоча програма розглянута та схвалена вченою радою факультету інформаційних технологій

Голова вченої ради факультету _____ Тетяна ГОВОРУЩЕНКО
Підпис Ім'я, ПРІЗВИЩЕ

Хмельницький 2024

КОМПЛЕКСНІ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ: ПРОЄКТУВАННЯ, ВПРОВАДЖЕННЯ, СУПРОВІД

Тип дисципліни	Обов'язкова
Рівень вищої освіти	Перший (бакалаврський)
Мова викладання	Українська
Семестр	Сьомий
Кредити ЄКТС	6,0
Форми навчання, для яких викладається дисципліна	Очна денна

Студент, який успішно завершив вивчення дисципліни, повинен: *аналізувати, виявляти та оцінювати* можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам та *проводити оцінку* ефективності та рівня захищеності ресурсів різних класів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах в ході проведення випробувань згідно встановленої політики інформаційної та\або кібербезпеки, *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; впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.), *реалізовувати* комплексні системи захисту інформації в автоматизованих системах (АС) організації (підприємства) відповідно до вимог нормативно-правових документів, *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 *використовувати* інформаційно-комунікаційні технології, сучасні методи і моделі інформаційної безпеки та/або кібербезпеки, *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; *використовувати* програмні та програмно-апаратні комплекси засобів захисту інформаційних ресурсів в інформаційно-телекомунікаційних (автоматизованих) системах, *вирішувати* завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами, та давати оцінку результативності якості прийнятих рішень, *застосовувати* методи та засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності, *забезпечувати* захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки, *вирішувати* задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах, *виконувати* моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки, *виявляти* небезпечні сигнали технічних засобів і *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, *інтерпретувати* результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик інформаційно-телекомунікаційних систем відповідно до вимог нормативних документів системи технічного захисту інформації; *виконувати* пошук, оброблення, аналіз та синтез інформації з різних джерел державною та іноземними мовами і *використовувати* отримані результати для ефективного рішення спеціалізованих задач дисципліни і професійної діяльності; *забезпечувати* введення підзвітності системи управління доступом до електронних інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах з використанням журналів реєстрації подій, їх аналізу та встановлених процедур захисту, ефективність професійної комунікації в задачах проєктування, впровадження та супроводу комплексних систем захисту інформації.

Зміст навчальної дисципліни. Основні поняття щодо проектування, впровадження та супроводу комплексних систем захисту інформації; класифікація загроз інформаційній безпеці. аналіз загроз на об'єкті захисту; типова структура та види технічних каналів витоку інформації: електричні, електромагнітні, акустичні, оптичні, побічні електромагнітні випромінювання; засоби блокування технічних каналів витоку інформації; фізична і апаратна безпека IoT; системи відеоспостереження; методи та засоби забезпечення систем фізичного доступу та охорони території; інструментарій для моніторингу процесів в інформаційно-телекомунікаційних системах.

Пререквізити: програмні і програмно-апаратні засоби захисту інформаційних систем від несанкціонованого доступу; електроніка і схемотехніка систем захисту; безпека безпроводових і мобільних технологій; безпека Web-ресурсів; проектно-технологічна практика; захист інформації в інформаційно-комунікаційних системах; прикладна криптологія; моделювання систем захисту даних, оцінка ризиків і прийняття рішень.

Кореквізити: переддипломна практика.

Запланована навчальна діяльність: лекції 34 год., лабораторних робіт 51 год., самостійної роботи 95 год. (в т.ч. курсовий проєкт 60 год.), разом 180 год.

Форми (методи) навчання: пояснювально-ілюстративні, практичні, проектні, продуктивні, проблемні, контекстні, застосування інформаційно-комп'ютерних технологій (САПР Solid Works тощо).

Форми оцінювання результатів навчання: усне опитування, письмова контрольна робота, захист курсового проекту, захист лабораторних робіт, підсумковий контрольний захід (семестровий контроль).

Вид семестрового контролю: іспит та курсовий проект.

Навчальні ресурси:

1. Технічні канали витоку інформації. Порядок створення комплексів технічного захисту інформації. Навчальний посібник / С.О. Іванченко, О.В. Гавриленко, О.А. Липський, А.С. Шевцов – К.: ІСЗЗІ НТУУ «КПІ», 2016. − 104 с.
2. Ластівка Г. І. Технічний захист інформації в інформаційних та телекомунікаційних системах: Навчальний посібник / Г. І. Ластівка, П. М. Шпатар – Чернівці: Чернівецький національний університет, 2018. - 252 с.
3. Методи і алгоритми захисту інформаційних ресурсів комп'ютерних систем: навчальний посібник / В. М. Джулій, Ю. П. Кльоц, І. В. Муляр, В. М. Чешун. – Хмельницький: ХмНУ, 2020. – 196 с.
4. Інформаційна безпека: навчальний посібник / [Ю. Я. Бобало, І. В. Горбатий, М. Д. Кіселичник, А. П. Бондарєв та ін.]; за заг. ред. д-ра техн. наук, проф. Ю. Я. Бобала та д-ра техн. наук, доц. І. В. Горбатого. – Львів: Видавництво Львівської політехніки, 2019. – 580 с.
5. Модульне середовище для навчання MOODLE. Доступ до ресурсу: https://msn.khmnu.edu.ua/.
6. Електронна бібліотека університету. Доступ до ресурсу: http://library.khmnu.edu.ua/.

Викладач: кандидат технічних наук, доцент Чешун В.М.

ВСТУП

Дисципліна «Комплексні системи захисту інформації: проєктування, впровадження, супровід» - одна з фундаментальних дисциплін професійної підготовки бакалаврів зі спеціальності „Кібербезпека”.

Мета дисципліни. Формування системи знань та розуміння предметної області необхідних для формалізованого опису, аналізу й синтезу комплексних систем захисту інформації; розв’язування складних спеціалізованих задач; застосування методів та засобів проектування, випробування, впровадження та супроводу комплексних систем захисту інформації.

Предмет дисципліни. Методи, методики, інформаційно-комунікаційні технології, програмно-апаратне забезпечення комплексних систем захисту інформації, їх впровадження та супроводу.

Завдання дисципліни. Забезпечити набуття компетентностей та досягнення програмних результатів навчання відповідно до Стандарту вищої освіти та освітньо-професійної програми підготовки бакалаврів зі спеціальності „Кібербезпека”:

компетентності:

КЗ 5. Здатність до пошуку, оброблення та аналізу інформації.

КФ 2. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки.

КФ 3. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах

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 впровадженої системи управління інформаційною та/або кібербезпекою.

КФ 11. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки.

КФ 12. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки.

результати навчання:

РН 3. Використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності

РН 14. Вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами, та давати оцінку результативності якості прийнятих рішень.

РН 16. Реалізовувати комплексні системи захисту інформації в автоматизованих системах (АС) організації (підприємства) відповідно до вимог нормативно-правових документів.

РН 18. Використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів.

РН 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.

РН 25. Забезпечувати введення підзвітності системи управління доступом до електронних інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних

(автоматизованих) системах з використанням журналів реєстрації подій, їх аналізу та встановлених процедур захисту.

РН 27. Вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах.

РН 28. Аналізувати та проводити оцінку ефективності та рівня захищеності ресурсів різних класів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах в ході проведення випробувань згідно встановленої політики інформаційної та\або кібербезпеки.

РН 29. 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.

РН 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.

РН 36. Виявляти небезпечні сигнали технічних засобів.

РН 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.

РН 38. Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик інформаційно-телекомунікаційних систем відповідно до вимог нормативних документів системи технічного захисту інформації.

РН 39. Проводити атестацію (спираючись на облік та обстеження) режимних територій (зон), приміщень тощо в умовах додержання режиму секретності із фіксуванням результатів у відповідних документах.

РН 40. Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів контролю характеристик ІТС відповідно до вимог нормативних документів системи технічного захисту інформації.

Студент, який успішно завершив вивчення дисципліни, повинен: *аналізувати, виявляти та оцінювати* можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам та *проводити оцінку* ефективності та рівня захищеності ресурсів різних класів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах в ході проведення випробувань згідно встановленої політики інформаційної та\або кібербезпеки, *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; впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.), *реалізовувати* комплексні системи захисту інформації в автоматизованих системах (АС) організації (підприємства) відповідно до вимог нормативно-правових документів, *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 *використовувати* інформаційно-комунікаційні технології, сучасні методи і моделі інформаційної безпеки та/або кібербезпеки, *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; *використовувати* програмні та програмно-апаратні комплекси засобів захисту інформаційних ресурсів в інформаційно-телекомунікаційних (автоматизованих) системах, *вирішувати* завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних

системах програмно-апаратними засобами, та давати оцінку результативності якості прийнятих рішень, *застосовувати* методи та засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності, *забезпечувати* захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки, *вирішувати* задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах, *виконувати* моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки, *виявляти* небезпечні сигнали технічних засобів і *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, *інтерпретувати* результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик інформаційно-телекомунікаційних систем відповідно до вимог нормативних документів системи технічного захисту інформації; *виконувати* пошук, оброблення, аналіз та синтез інформації з різних джерел державною та іноземними мовами і *використовувати* отримані результати для ефективного рішення спеціалізованих задач дисципліни і професійної діяльності; *забезпечувати* введення підзвітності системи управління доступом до електронних інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах з використанням журналів реєстрації подій, їх аналізу та встановлених процедур захисту, ефективність професійної комунікації в задачах проєктування, впровадження та супроводу комплексних систем захисту інформації.

СТРУКТУРА ЗАЛІКОВИХ КРЕДИТІВ ДИСЦИПЛІНИ

Назва теми	Кількість годин, відведених на:		
	лекції	**лабораторні роботи**	**самостійну роботу***
Сьомий семестр			
Тема 1. Проєктування комплексних систем захисту інформації	6	8	26
Тема 2. Технічні засоби захисту інформації	20	16	52
Тема 3. Випробування та впровадження комплексної системи захисту інформації	6	8	27
Тема 4. Супровід комплексної системи захисту інформації	2	2	7
Разом:	**34**	**34**	**112***

*Самостійна робота включає час на виконання курсового проєкту загальним обсягом 60 год

ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Зміст лекційного курсу

Номер лекції	Перелік тем лекцій, їх анотації	Кількість годин
	Сьомий семестр	
	Тема 1. Проектування комплексних систем захисту інформації	
1	**Загальні положення про комплексні системи захисту інформації** Структура та зміст дисципліни і методичні рекомендації щодо її вивчення. Місце дисципліни у навчальному процесі. Вимоги до знань та вмінь тих, хто навчається. Характеристика рекомендованих під час вивчення дисципліни джерел інформації. Використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки. Визначення, позначення та скорочення. Поняття та призначення комплексної системи захисту інформації. Основні вимоги до КСЗІ. Принципи та етапи захисту від загроз при побудові КСЗІ**.** Літ.:[1] с.6-8; [2] с.81-86; [3] с.500-515; [10] с.1-48; [11] с.2-13; [17]	2
2	**Основні принципи організації КСЗІ** Принципи організації КСЗІ. Концептуальні підходи до проєктування систем захисту. Порядок проведення робіт із створення КСЗІ в інформаційно-телекомунікаційній системі (ІТС). Етапи створення КСЗІ в ІТС. Формування технічного завдання на створення КСЗІ в ІТС. Базові розділи ТЗ. Нормативний супровід розробки ТЗ. Вимоги НД ТЗІ 3.7-001-99 до змісту, послідовності та викладення розділів ТЗ на створення КСЗІ в ІКС. Розробка ескізного проєкту КСЗІ. Представлення схем, структур, елементів КСЗІ. Оформлення та представлення текстової документації. Розробка комплекту документації для етапу проєктування КСЗІ. КСЗІ в критичній інфраструктурі. Літ.:[1] с.6-16; [2] с.189-199; [10] с.19-49; [11] с.13-25; [16]; [17]; [18]	2
3	**Класифікація загроз інформаційній безпеці. Аналіз загроз на об'єкті захисту** Класифікація загроз інформаційній безпеці, ознаки класифікації. Ознаки моделі порушника, як етапу побудови КСЗІ. Категорії порушників. Класифікація порушника. Поняття контрольована зона. Модель загроз для ідентифікації каналів витоку інформації. Джерело загрози. Перелік загроз з визначенням порушень властивостей інформації та ІТС. Літ.:[3] с.19-27; [4] с.20-37; [6] с.12-22; [10] с. 49-67; [11] с. 27-42	2
	Тема 2. Технічні засоби захисту інформації	
4	**Джерела та носії інформації** Характеристика захищеної інформації. Захист інформації як інтегральна проблема та шляхи її вирішення. Специфіка застосування програмно-апаратних засобів захисту в СКЗІ, оцінка результативності якості прийнятих рішень щодо їх застосування. Умови безпеки інформації. Небезпечні сигнали і їх джерела. Класифікація джерел та носіїв інформації. Сутність запису і знімання інформації з носія. Джерела сигналів. Джерела функціональних сигналів. Побічні електромагнітні випромінювання (ПЕМВ) та наведення. Програмні та програмно-апаратні комплекси виявлення вторгнень. Літ.:[1] с.11-22; [2] с.79-86; [3] с.27-33; [4] с.20-37; [11] с.66-88	2
5	**Типова структура та види технічних каналів витоку інформації (ТКВІ).** Загальна характеристика технічного каналу витоку інформації. Класифікація та характеристика технічних каналів витоку інформації. Особливості витоку інформації технічними каналами. Типова структура та види технічних каналів витоку інформації. Схема можливих каналів витоку і несанкціонованого доступу до інформації. Літ.:[1] с.17-26; [2] с. 18-34; [3] с.516-527	2

6	**Методи та засоби захисту від витоку інформації** Використання програмних та програмно-апаратних комплексів захисту інформаційних ресурсів Заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах. Принципи блокування ТКВІ. Заходи щодо блокування ТКВІ з використанням активних та пасивних засобів. Заходи щодо виявлення портативних електронних пристроїв перехоплення інформації.Заходи щодо перетворення сигналів у каналах зв'язку. Літ.:[2] с.148-186; [3] с.31-38; [6] с.70-86; [30]	2
7	**Електричні канали витоку інформації** Класифікація електричних каналів витоку інформації. Забезпечення захисту інформації від ненавмисної дії технічними засобами. Виявлення небезпечних сигналів технічних засобів. Екранування технічних засобів. Заземлення. Літ.:[1] с.26-44; [2] с. 46-63 [[3] с.328-343	2
8	**Електромагнітні канали витоку інформації** Види побічних електромагнітних випромінювань. Канал побічних електромагнітних випромінювань основних та додаткових технічних засобів. Підходи до зняття інформації через електромагнітні випромінювання. Канал “паразитної” модуляції сигналів ВЧ генераторів. Канал “паразитної” ВЧ генерації підсилювачів. Канал побічних електромагнітних наведень на лінії електроживлення (заземлення) та комунікації. Канал ВЧ нав’язування (для зняття інформації, що обробляється. Літ.:[1] с.34-46; [2] с.83-90; [3] с.328-343	2
9	**Радіоканали втрат інформації** Структура радіоканалів втрат інформації. Класифікація технічних каналів витоку акустичної (мовної) інформації. Акустичні канали витоку інформації. Віброакустичні канали витоку інформації. Акустоелектричні канали. Акустооптоелектронні (лазерні акустичні) канали витоку інформації. Канали ВЧ нав’язування (для зняття мовної інформації). Перехоплення акустичних сигналів. Літ.:[1] с.45-76, 132-148; [[2] с.34-46, с.117-142	2
10	**Технічні канали витоку інформації на основі закладних пристроїв** Сутність та класифікація засобів несанкціонованого перехоплення інформації (закладних пристроїв). Загальні характеристики та особливості деяких типів закладних пристроїв. Пристрої прослуховування приміщень. Радіозакладні пристрої. Заходи захисту інформації від витоку каналами на основі закладних пристроїв Літ.:[1] с.56-76, 132-148; [2] с.117-142	2
11	**Системи блокування відеоспостереження** Методи та засоби відеоспостереження. Принципи протидії засобам відеорозвідки. Класифікація візуально-оптичних каналів витоку інформації. Методи . захисту інформації від витоку по візуально-оптичному каналу. Методи і засоби пошуку прихованих відеокамер. Пошук і блокування прихованих пристроїв відеоспостереження, що використовують радіоканал для передачі інформації Літ.:[1] 126-128; [2] с.63-67; [3] с.506-527	2
12	**Канали витоку інформації при експлуатації ЕОМ** Види і природа каналів витоку інформації при експлуатації ЕОМ. Способи і методи ЗІ, оброблюваної засобами електронної техніки, від витоку радіочастотним каналу. Механізм виникнення ПЕМВ засобів цифрової електронної техніки. Технічна реалізація пристроїв маскування. Оцінка рівня ПЕМВ. Прилади виявлення ПЕМВ. Літ.: [1] с.70-81; [2] с.79-109; [3] с.516-521	2

13	**Фізична і апаратна безпека IoT** Вступ. Терміни та визначення безпеки Інтернету речей. Загальновживані поняття кібербезпеки. Анатомія кібератак на IoT-пристрої. Фізична і апаратна безпека. Корінь довіри. Адресний простір в процесорі і пам'яті. Безпека зберігання даних. Застосування технологій розумного будинку фірми Xiaomi в системах комплексного захисту. Літ.: [5] с.62-108; [9] с.4-110; [24]; [28]	2
14	**Методи та засоби забезпечення систем фізичного доступу та охорони території** Системи фізичного захисту об'єктів. Типова система фізичного доступу. Доглядові системи.. Ручні та арочні металошукачі. Автономні та мережеві системи доступу. Сигналізації. Літ [2] с.199-250; [3] с.527-548; [10] с.67-101	2
Тема 3. Випробування та впровадження комплексної системи захисту інформації		
15	**Організація випробувань КСЗІ** Реалізація КСЗІ відповідно до вимог нормативно-правових документів. Введення КСЗІ в дію. Аналіз та оцінка ефективності та рівня захищеності ресурсів різних класів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах в ході проведення випробувань згідно встановленої політики інформаційної та\або кібербезпеки. Підготовка КСЗІ до введення в дію. Комплектування КСЗІ. Монтажно-пусковий період. Пуско-налагоджувальні роботи. Попередні випробування та дослідна експлуатація. Оцінка ефективності та рівня захищеності ресурсів в ході проведення випробувань згідно встановленої політики інформаційної та\або кібербезпеки. Літ.: [1] с.81-91; [2] с.189-198; [3] с.548-562; [11] с.111-123; [16] ; [17]; [18]	2
16	**Державна експертиза КСЗІ в ІТС** Положення про державну експертизу в сфері ТЗІ**.** Порядок організації та проведення експертизи**.** Порядок надання Експертного висновку та Атестату**.** Особливості проведення експертиз КСЗІ державними органами**.** Особливості проведення експертизи шляхом декларації Літ.: [1] с.91-99; [11] с.124-123; [16] ; [17]; [18]	2
Тема 4. Супровід комплексної системи захисту інформації		
17	**Супровід КСЗІ** План робіт із захисту інформації в ІТС. Контрольно-профілактичні заходи. Інженерно-технічні заходи. Задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем. Кадрові заходи. Забезпечення супроводу КСЗІ в ІКС. Контроль встановленого порядку оброблення інформації в ІКС. Основні вимоги до КЗЗ від НСД. НД ТЗІ 1.1-00299: безперервний захист, атрибути та диспетчер доступу, реєстрація дій, функції та механізми захисту, забезпечення послуг безпеки та гарантій їх реалізації. Вирішення задачі супроводу КСЗІ. Особливості супроводу КСЗІ в ІТС державних установ. Державний контроль за станом ТЗІ Літ.: [3] с.562-566; [11] с.134-154; [16] ; [17]; [18]	2
	Разом:	**34**

Зміст лабораторних робіт

№ з/п	Тема лабораторного заняття	Кількість годин
	Сьомий семестр	
1	Аналіз структури об'єкту захисту та оцінка можливих загроз, уразливостей та дестабілізуючих чинників. Літ.:[1] с.6-16; [2] с.189-199; [3] с.19-27; [4] с.20-37; [6] с.12-22; [10] с. 49-67; [11] с.13-42; [15]; [16]; [17]; [29]	4
2	Розроблення моделі порушника та загроз і реалізація політики інформаційної безпеки як етап проєктування КСЗІ. Літ.:[3] с.19-27; [4] с.20-37; [6] с.12-22; [10] с. 49-67; [11] с. 27-42; [30]	4
3	Дослідження характеристик технічних засобів прослуховування інформації. Використання генераторів шуму для блокування витоку інформації. Літ.:[1] с.17-44; [2] с. 18-63, 83-90; [3] с.328-343, 516-527	4
4	Організація та використання систем відеомоніторингу контрольованої території. Літ.:[1] с.70-81, 126-128; [2] с.63-67; [3] с.506-527	4
5	Утворення системи контролю і захисту приміщень на основі IoT пристроїв Xiaomi (модулів розумного будинку) та давачів охоронної сигналізації. Літ.: [2] с.199-250; [3] с. 527-548; [5] с.62-108; [9] с.10-80; [10] с.67-101; [24]; [28]	4
6	Виявлення і вимірювання параметрів небезпечних сигналів та локалізація їх джерел. Методика та засоби виявлення закладних пристроїв. Літ.: [1] с.60-76; [2] с.87-138; [19]; [20]	4
7	Оцінка ефективності та рівня захищеності КСЗІ, документальний супровід КСЗІ (протокол випробувань комплексних систем захисту інформації, документація на етапі експлуатації КСЗІ) Літ.: [1] с.81-99; [2] с.189-198; [3] с.548-562; [11] с.111-123; [16] ; [17]; [18]; [21]; [24]	4
8	Впровадження та забезпечення функціонування комплексних систем захисту інформації, моніторинг роботи та технічний супровід. Літ.: [3] с.562-566; [11] с.134-154; [16] ; [17]; [18]	4
9	Підсумкове заняття. Контрольна робота	2
	Разом:	**34**

Зміст самостійної (у т.ч. індивідуальної) роботи

На самостійне опрацювання студентів виноситься опрацювання лекційного матеріалу, підготовка до виконання і захисту лабораторних робіт, виконання та підготовка до захисту курсового проєкту. Керівництво самостійною роботою та виконанням завдань здійснює викладач згідно з розкладом консультацій в позаурочний час, в тому числі із застосуванням технологій інтерактивного та дистанційного навчання.

Номер тижня	Вид самостійної роботи	Кількість годин
1	Опрацювання теоретичного матеріалу. Отримання завдання на КП, підготовка до виконання ЛР1	6
2	Опрацювання теоретичного матеріалу, підготовка до захисту ЛР1.	7
3	Опрацювання теоретичного матеріалу, робота над КП, підготовка до виконання ЛР2	6
4	Опрацювання теоретичного матеріалу, підготовка до захисту ЛР2	7
5	Опрацювання теоретичного матеріалу, робота над КП, підготовка до виконання ЛР3	6
6	Опрацювання теоретичного матеріалу, підготовка до захисту ЛР3	7
7	Опрацювання теоретичного матеріалу, робота над КП, підготовка до виконання ЛР4	6
8	Опрацювання теоретичного матеріалу, підготовка до захисту ЛР №4	7
9	Опрацювання теоретичного матеріалу, робота над КП, підготовка до виконання ЛР5	7
10	Опрацювання теоретичного матеріалу, підготовка до виконання і захисту ЛР5	7
11	Опрацювання теоретичного матеріалу, робота над КП, підготовка до виконання ЛР6	6
12	Опрацювання теоретичного матеріалу, підготовка до захисту ЛР6	7
13	Опрацювання теоретичного матеріалу, робота над КП, підготовка до виконання ЛР7	6
14	Опрацювання теоретичного матеріалу, підготовка до захисту ЛР7	7
15	Опрацювання теоретичного матеріалу, Підготовка до захисту КП, підготовка до виконання ЛР8	6
16	Опрацювання теоретичного матеріалу, підготовка до захисту ЛР8	7
17	Опрацювання теоретичного матеріалу. Підготовка до КР.	7
	Разом:	**112**

Умовні позначення: ЛР – лабораторна робота, КП – курсовий проєкт, КР – контрольна робота

Навчальним планом дисципліни передбачено курсовий проект, на виконання якого виділяється 2 кредити ЄКТС (60 год.) самостійної роботи студента під керівництвом викладача та з консультуванням за графіком.

Згідно з навчальним планом підготовки бакалаврів за спеціальністю «Кібербезпека» курсовий проєкт виконується у 7 семестрі поетапно, відповідно до календарного плану.

Завдання на курсовий проєкт базується на матеріалі, який опрацьовується під час лекційних, лабораторних та самостійних занять в ході вивчення дисципліни. Тематика курсового проєкту пов’язана з майбутньою спеціальністю студентів. В курсовому проєкті студент повинен показати свої знання в галузі проєктування комплексних систем захисту інформації в кіберпросторі. Крім того, в якості об’єкту для курсового проєкту можуть бути дослідження та впровадження відомих технології проєктування засобів захисту, реалізація тестових програм тощо.

Календарний план виконання курсового проєкту

Зміст етапу	Термін виконання
1 Вибір та затвердження теми курсового проєкту; розробка завдання на курсовий проєкт; складання календарного графіка виконання курсового проєкту	1-2 тиждень
2 Аналіз об'єкта захисту та аналіз захищеності його інформації від несанкціонованого втручання	3-4 тиждень
3 Аналіз та опис наявної системи захисту інформації	5-8 тиждень
4 Проєктування пропонованої КСЗІ	9-12 тиждень
5 Написання тексту пояснювальної записки та розробка графічних матеріалів	13-14 тиждень
6 Остаточне коригування курсового проєкту з урахуванням зауважень керівника; оформлення курсового проєкту, як документа відповідно до вимог	15 тиждень
7 Підготовка до захисту та захист курсового проєкту	16 тиждень

Об’єктом дослідження для курсового проєкту рекомендується обрати підприємство, на якому студент проходив проєктно-технологічну практику. Заохочуються пропозиції студентів щодо самостійного, за узгодженням з викладачем, вибору теми курсового проєкту. Самостійний вибір предметної області, в якій доцільно створювати КСЗІ, дозволяє зробити висновок щодо рівня творчої активності студента, його вміння самостійно здійснити попередній аналіз предметної області і розробити технічне завдання.

При виконанні курсового проєкту обов’язково повинні бути використані такі елементи:

- аналіз об’єкта захисту відповідно до НД ТЗІ 3.7-001-2005;
- розробка моделі загроз;
- розробка моделі порушника;
- розробка політики безпеки;
- аналіз інженерно-технічних, апаратних та програмних засобів захисту інформації;
- синтез оптимальної КСЗІ;
- розробка документації на етапах впровадження і супроводу.

Розробка повинна бути представлена у вигляді моделі КСЗІ і супроводжуватись пояснювальною запискою, яка б повинна бути обсягом ***50-60 сторінок*** і рекомендовано містила в собі такі елементи:

- загальний аналіз об’єкта захисту, аналіз концептуальних вимог та інформаційних потреб для конкретної предметної області;
- виявлення інформаційних об’єктів та зв’язків між ними;
- побудова концептуальної схеми предметної області;
- аналіз загроз та ризиків для інформаційно-комунікаційної системи підприємства, оцінка ступеню загрози інформації, що захищається;
- моделювання можливих каналів витоку інформації;
- аналіз інженерно-технічних, апаратних та програмних засобів захисту інформаційних ресурсів підприємства та вибір оптимальних;
- розробка технічного завдання для системи захисту
- технічний проєкт системи захисту щодо розробки загальних рішень по системі та її частинах, функціональній і організаційних структурах, функціях персоналу, по структурі та складу технічних засобів, постановках і алгоритмах розв’язання задач, мовах, які застосовуються, по організації та веденню бази даних, системі класифікації та кодування інформації, програмному забезпеченню, розробці плану організаційних заходів щодо підготовки об’єкта до введення системи в дію, по правовому забезпеченню;
- робочий проєкт системи захисту, який включає програмно-апаратну реалізацію системи захисту та оформлення відповідної робочої документації;

- розробка заходів з технічного захисту інформації на об'єкті захисту;
- розробка моделі охоронної та пожежної сигналізації об'єкта (приміщення), систтеми відеоспостереження, тощо.
- розрахунок зон поширення акустичних і електромагнітних хвиль з об'єкта захисту з масштабною прив'язкою на місцевості;
- аналіз роботи та випробовування розробленої системи захисту та доведення ефективності та коректності її функціонування;
- оцінка ступеня захисту інформації на об'єкті;
- розробку відповідної документації на етапі впровадження і супроводу;
- формулювання рекомендацій по роботі з засобом (інструкції з технічного обслуговування, інструкції системному адміністратору, інструкції користувачу- оператору).

Вибір необхідних розділів курсового проєкту узгоджується з керівником і повинен бути адаптований до тематики курсового проєкту.

Як результат виконання курсового проєкту є розробка графічної частини, яка демонструє основні результати виконаної розробки ***(5 креслень)***

В курсовому проєкті обов'язковими є два креслення:

1) Схема інформаційних потоків;
2) Схема структурна КСЗІ ІТС підприємства.

Інші вибираються довільно, щоб розкрити суть проєкту, напрклад:

- схему структурну мережі підприємства;
- модель загроз;
- модель порушника;
- алгоритм захисту мережі підприємства;
- схему роботи системи захисту;
- рівні інтеграції різних елементів інтегрованої КСЗІ;
- алгоритми обчислень в системі;
- архітектуру системи захисту
- структурну схема охоронно-пожежної сигналізації:
- структурну схему системи відеонагляду, тощо.

ТЕХНОЛОГІЇ ТА МЕТОДИ НАВЧАННЯ

Процес навчання з дисципліни ґрунтується на використанні традиційних та сучасних методів, зокрема: лекції проводяться з використанням пояснювально-ілюстративних та проблемних методів, лабораторні роботи проводяться з використанням практичних, продуктивних, проблемних, контекстних методів та з застосуванням інформаційно-комп'ютерних технологій (САПР Solid Works тощо), курсове проектування здійснюється з використанням проектних, проблемних та контекстних методів.

Застосовувані при викладанні дисципліни методи навчання сприяють розвитку у студентів навичок soft skills: спілкування з проблемних питань під час лекцій, захист курсового проекту, прилюдні захисти лабораторних робіт з обґрунтуванням прийнятих рішень щодо вибору методів рішення завдань в діалозі з викладачем і групою сприяють формуванню і удосконаленню вмінь публічних виступів, емпатичного слухання, відстоювання власної точки зору, самоаналізу і самокритики; адаптованість, вміння користуватися інтернет-ресурсами та іншими джерелами інформації, синтезувати та критично осмислювати інформацію з різних джерел передбачені специфікою дисципліни, що передбачає рішення проблемних завдань із застосуванням творчих підходів; обмежений час на виконання лабораторних робіт, контрольних завдань, чітко визначені і надані в силабусі терміни проходження контрольних точок і відпрацювання заборгованостей сприяють розвитку пунктуальності, здатності до самоорганізації та управління часом (тайм-менеджменту).

При вивченні дисципліни можуть бути зараховані результати навчання, здобуті у неформальній освіті. Визнання результатів навчання, здобутих у неформальній освіті, реалізується згідно з чинним законодавством і регулюється Положенням про порядок перезарахування результатів навчання та визначення академічної різниці у ХНУ https://www.khnu.km.ua/root/files/01/10/03/006.pdf.

МЕТОДИ КОНТРОЛЮ

Поточний контроль здійснюється під час лабораторних занять, а також у дні проведення контрольних заходів, встановлених робочим планом дисципліни.

При цьому використовуються такі методи поточного контролю:

- усне опитування;
- захист лабораторних робіт;
- письмова контрольна робота.

Семестровий контроль проводиться у формі іспиту та курсового проекту. При виведенні підсумкової семестрової оцінки враховуються результати як поточного контролю, так і підсумкового контрольного заходу.

ОЦІНЮВАННЯ РЕЗУЛЬТАТІВ НАВЧАННЯ СТУДЕНТІВ

Оцінювання академічних досягнень студента здійснюється відповідно до «Положення про контроль і оцінювання результатів навчання здобувачів вищої освіти у ХНУ». Кожний вид роботи з дисципліни оцінюється за інституційною чотирибальною шкалою. Семестрова підсумкова оцінка визначається як середньозважена з усіх видів навчальної роботи, виконаних і зданих позитивно з урахуванням коефіцієнта вагомості. Вагові коефіцієнти змінюються залежно від структури дисципліни і важливості окремих видів її робіт.

Структурування дисципліни за видами робіт і оцінювання результатів навчання студентів у семестрі за ваговими коефіцієнтами

	Аудиторна робота	**Контрольні заходи**	**Підсумковий контрольний захід**
Вид заняття	Лабораторні роботи	Контрольна робота	Семестровий контроль (іспит)
Тема	1-4	1-4	1-4
Ваговий коефіцієнт	0,4	0,2	0,4

Оцінювання лабораторних робіт. Оцінка, яка виставляється за лабораторне заняття, складається з таких елементів: усне опитування студентів перед допуском до виконання лабораторної роботи; знання теоретичного матеріалу з теми; якість оформлення протоколу і звіту; вільне володіння студентом спеціальною термінологією і уміння професійно обґрунтувати прийняті рішення; своєчасний захист лабораторної роботи.

Термін захисту звіту з лабораторної роботи вважається своєчасним, якщо студент захистив її в день виконання або на наступному після виконання роботи занятті. Пропущене лабораторне заняття студент зобов'язаний відпрацювати в лабораторіях кафедри у встановлений викладачем термін з реєстрацією у відповідному журналі кафедри, але не пізніше, ніж за два тижні до кінця теоретичних занять у семестрі.

Оцінку за лабораторне заняття викладач оголошує одразу після захисту звіту з лабораторної роботи і проставляє в електронний журнал дисципліни.

Оцінювання контрольної роботи. Контрольна робота складається з теоретичного питання та практичного завдання. Оцінювання здійснюється за чотирибальною шкалою.

Оцінку «відмінно» отримує студент який дав повну письмову відповідь на теоретичне питання та правильно виконав поставлене практичне завдання.

Оцінку «добре» отримує студент, який допустив дві-три несуттєві помилки при відповіді на теоретичне питання та правильно виконав поставлене практичне завдання.

Оцінку «задовільно» отримує студент, який дав лише часткову відповідь на теоретичне питання або допустив суттєві помилки при виконанні практичного завдання.

Оцінку «незадовільно» отримує студент, який не зміг виконати практичне завдання або не дав відповіді на теоретичне питання.

Оцінку за контрольну роботу викладач проставляє в електронний журнал дисципліни не пізніше ніж через десять днів після проведення контрольного заходу.

Оцінювання курсового проєкту.

При оцінюванні курсового проєкту враховується дотримання в ній ряду вимог. Виконання курсового проєкту передбачає ґрунтовне вивчення літературних джерел з обраної теми, теоретичні знання та практичні навички, аналізу особисто зібраного фактичного матеріалу, або опрацювання матеріалів інших дослідників, власне творче бачення студента.

При захисті курсового проєкту комісія оцінює якість та вчасність виконання кожного з етапів виконання курсового проєкту.

Структурування курсового проєкту за видами робіт і оцінювання результатів навчання студентів у семестрі за ваговими коефіцієнтами

1 розділ записки	2 розділ записки	3 розділ записки	4 розділ записки	Реалізація	Креслення / графічна документація	Захист КП
ВК: 0.1	ВК: 0.1	ВК: 0.1	ВК: 0.15	ВК: 0.2	ВК: 0.15	ВК: 0.2

При проведенні захисту та оцінюванні курсового проекту необхідно керуватися такими критеріями.

Оцінку "***відмінно***" (шкала ECTS – A) отримує студент за глибоке і повне опанування понятійного апарату та матеріалу, в якому він легко орієнтується; уміння зв'язувати теорію з практикою, вирішувати практичні завдання, висловлювати і обґрунтовувати свої судження. Відмінна оцінка виставляється за якісне оформлення звіту, грамотний і логічний виклад відповіді під час захисту. Студент не повинен вагатися при видозміні запитання, повинен робити детальні та узагальнюючі висновки.

Оцінку "***добре***" (шкала ECTS – B) отримує студент за повне засвоєння навчального матеріалу, володіння понятійним апаратом, орієнтування в вивченому матеріалі, свідоме використання знань для вирішення практичних завдань, грамотний виклад відповіді, але у змісті і формі відповіді (або звіту) наявні окремі неточності (похибки), нечіткі формулювання закономірностей тощо. Відповідь студента повинна будуватись на основі самостійного мислення.

Оцінку "***добре***" (шкала ECTS – C) отримує студент за правильну відповідь і якісне оформлення звіту, в сукупності яких фіксується дві–три суттєвих помилки.

Оцінку "***задовільно***" (шкала ECTS – D) заслуговує студент, який за результатами практики виявив знання основного навчально-програмного матеріалу в обсязі, необхідному для подальшої практичної діяльності за професією, що справляється з виконанням практичних завдань, передбачених програмою практики. Як правило, відповідь студента будується на рівні репродуктивного мислення, він слабо знає структуру курсу, допускає помилки у відповіді, засвоїв і набув практичних навичок у проєктуванні типових систем захисту, але допустив неточності, не має чіткого поняття про зв'язок сучасних технологій з практичним застосуванням, що відзначається також і на якості звіту з практики. Вагається при відповіді на видозмінене запитання, але разом з тим володіє знаннями, що дозволяють йому під керівництвом викладача усунути неточності у відповіді.

Оцінку "***задовільно***" (шкала ECTS – E), заслуговує студент за виявлене під час виконання КП неповне опанування програмного матеріалу, але з відповіді якого слідує, що отримані ним знання і набуті практичні навички з розробки систем захисту відповідають мінімальним критеріям оцінювання.

Оцінка **"*незадовільно*"** (шкала ECTS – FX) виставляється, коли студент має розрізнені, безсистемні знання, не вміє виділяти головне і другорядне, допускається помилок у визначенні понять КП, перекручує їх зміст, хаотично і невпевнено викладає матеріал, не може використовувати знання при вирішенні практичних завдань. Як правило, оцінка "незадовільно" виставляється студенту, який за результатами виконання КП показує, що не може продовжити навчання без додаткових знань.

Оцінка "***незадовільно***" (шкала ECTS – F) якщо курсовий проєкт виконаний не у повному обсязі та з відхиленням від визначеної тематики. Проєкт не відповідає встановленим вимогам, містить грубі помилки, під час захисту курсового проєкту студент не дав відповіді на більшість поставлених запитань.

Семестровий контроль (іспит). Підсумковий контрольний захід з дисципліни проводиться в формі іспиту. Екзаменаційний білет складається з двох теоретичних питань і задачі. Під час іспиту за наданими відповідями і рішеннями (розв'язками) виконується оцінювання рівня засвоєння студентом матеріалу дисципліни.

Оцінка за підсумковий контрольний захід проставляється викладачем в електронний журнал дисципліни в день здачі іспиту і враховується в автоматизованому режимі при визначенні підсумкової семестрової оцінки студента з дисципліни за інституційною шкалою і шкалою ЄКТС

Засвоєння студентом теоретичного матеріалу з дисципліни оцінюється за наведеними в таблиці критеріями.

Критерії оцінювання знань студентів

Оцінка за інституційною шкалою	**Узагальнений критерій**
1	*2*
Відмінно	Студент глибоко і у повному обсязі опанував зміст навчального матеріалу, легко в ньому орієнтується і вміло використовує понятійний апарат; уміє пов'язувати теорію з практикою, вирішувати практичні завдання, впевнено висловлювати і обґрунтовувати свої судження. Відмінна оцінка передбачає, логічний виклад відповіді державною мовою (в усній або у письмовій формі), демонструє якісне оформлення роботи і володіння спеціальними інструментами. Студент не вагається при видозміні запитання, вміє робити детальні та узагальнюючі висновки. При відповіді допустив дві-три несуттєві похибки.
Добре	Студент виявив повне засвоєння навчального матеріалу, володіє понятійним апаратом і фаховою термінологією, орієнтується у вивченому матеріалі; свідомо використовує теоретичні знання для вирішення практичних задач; виклад відповіді грамотний, але у змісті і формі відповіді можуть мати місце окремі неточності, нечіткі формулювання закономірностей тощо. Відповідь студента будується на основі самостійного мислення. Студент у відповіді допустив дві - три несуттєві помилки.
Задовільно	Студент виявив знання основного програмного матеріалу в обсязі, необхідному для подальшого навчання та практичної діяльності за професією, справляється з виконанням практичних завдань, передбачених програмою. Як правило, відповідь студента будується на рівні репродуктивного мислення, студент має слабкі знання структури курсу, допускає неточності і суттєві помилки у відповіді, вагається при відповіді на видозмінене запитання. Разом з тим, набув навичок, необхідних для виконання нескладних практичних завдань, які відповідають мінімальним критеріям оцінювання і володіє знаннями, що дозволяють йому під керівництвом викладача усунути неточності у відповіді.
Незадовільно	Студент виявив розрізнені, безсистемні знання, не вміє виділяти головне і другорядне, допускається помилок у визначенні понять, перекручує їх зміст, хаотично і невпевнено викладає матеріал, не може використовувати знання при вирішенні практичних завдань. Як правило, оцінка "незадовільно" виставляється студенту, який не може продовжити навчання без додаткової роботи з вивчення дисципліни.

Якщо студент отримав негативну оцінку за певним видом робіт, то він має перездати її в установленому порядку, але обов'язково до терміну наступного контролю.

У випадку, коли студент не виконав індивідуальний план з дисципліни у заплановані терміни без поважних причин, то під час відпрацювання заборгованості при позитивній відповіді йому виставляється оцінка „задовільно".

Студент, який у встановлені терміни не виконав індивідуальний план поточної роботи з дисципліни повністю або частково, до здачі підсумкового контрольного заходу не допускається.

Студент, який набрав позитивний середньозважений бал за поточну роботу і не здав підсумковий контрольний захід (іспит), вважається невстигаючим.

Підсумкова семестрова оцінка за інституційною шкалою і шкалою ЄКТС встановлюється в автоматизованому режимі після внесення викладачем усіх оцінок до електронного журналу.

Співвідношення вітчизняної шкали оцінювання і шкали оцінювання ЄКТС

Оцінка ЄКТС	**Інституційна інтервальна шкала балів**	**Інституційна оцінка, критерії оцінювання**	
A	4,75–5,00	5	***Відмінно*** – глибоке і повне опанування навчального матеріалу і виявлення відповідних умінь та навиків
B	4,25–4,74	4	***Добре*** – повне знання навчального матеріалу з кількома незначними помилками
C	3,75–4,24	4	***Добре*** – в загальному правильна відповідь з двома-трьома суттєвими помилками
D	3,25–3,74	3	***Задовільно*** – неповне опанування програмного матеріалу, але достатнє для практичної діяльності за професією
E	3,00–3,24	3	***Задовільно*** – неповне опанування програмного матеріалу, що задовольняє мінімальні критерії оцінювання
FX	2,00–2,99	2	***Незадовільно*** – безсистемність одержаних знань і неможливість продовжити навчання без додаткових знань з дисципліни
F	0,00–1,99	2	***Незадовільно*** – необхідна серйозна подальша робота і повторне вивчення дисципліни

ПИТАННЯ ДЛЯ САМОКОНТРОЛЮ ЗДОБУТИХ СТУДЕНТАМИ РЕЗУЛЬТАТІВ НАВЧАННЯ

1. Організаційні основи розробки проектів, реалізації та модернізації захищених інформаційних і комунікаційних систем.
2. Соціальні та морально етичні норми колективного розроблення проектів.
3. Правові норми організації роботи колективу для розробки проектів.
4. Оптимізація співробітництва у колективі при розробці проектів.
5. Загальна технологія розробки комплексів засобів захисту інформаційно-комунікаційних систем.
6. Індикатори електромагнітних випромінювань.
7. Радіочастотоміри.
8. Автоматизовані пошукові комплекси.
9. Мобільні пошукові комплекси.
10. Скануючі приймачі.
11. Спеціалізоване програмне забезпечення.
12. Тепловізорні засоби.
13. Стаціонарні комплекси автоматичного виявлення радіомікрофонів.
14. Типові методи та прийоми проектування захищених інформаційних та комунікаційних систем.
15. Засоби захисту для складових КСЗІ.
16. Класифікація джерел~~а~~ загроз та загроз~~н~~ інформації.
17. Сутність технічного каналу витоку інформації.
18. Загальна класифікація каналів витоку інформації.
19. Електромагнітні канали витоку інформації.
20. Електричні канали витоку інформації.
21. Параметричні канали витоку інформації.
22. Повітряні канали витоку акустичної інформації.
23. Вібраційні канали витоку акустичної інформації.
24. Електроакустичні канали витоку акустичної інформації.
25. Оптико-електронний канал витоку акустичної інформації, його характеристика, методи блокування.
26. Індукційний метод перехоплення інформації при її передачі по каналах зв’язку.
27. Класифікація, принцип роботи акустичних закладок.
28. Класифікація, принцип роботи віброакустичних закладок.
29. Класифікація, принцип роботи спрямованих мікрофонів.
30. Класифікація, принцип роботи панорамних скануючих приймачів.
31. Класифікація, принцип роботи аналізаторів спектру та пеленгаторів.
32. Програмно-апаратні комплекси радіо-, радіотехнічної розвідки.
33. Засоби візуальної розвідки.
34. Системи спостереження за транспортними засобами. Радіомаяки. Радіонавігаційний приймач.
35. Класифікація методів та засобів захисту інформації від витоку технічними каналами.
36. Засоби виявлення, локалізації і нейтралізації закладних пристроїв.
37. Основні вимоги до структури і параметрів засобів радіомоніторингу при захисті мовної інформації.
38. Пасивні методи та засоби захисту інформації.
39. Активні методи та засоби захисту інформації.
40. Методи та засоби виявлення та подавлення диктофонів.
41. Методи і засоби пошуку електронних закладних засобів.
42. Методи пошуку закладок з використанням індикаторів поля, інтерсепторів і радіочастотомірів.
43. Методи пошуку закладок з використанням нелінійних локаторів, виявлячі порожнеч

(пустот), металошукачів і рентгенівських апаратів
44. Засоби пошуку пристроїв перехоплення інформації. Сканерні приймачі й аналізатори спектру.
45. Програмно-апаратні та спеціальні комплекси контролю сигналів.
46. Засоби пошуку пристроїв перехоплення інформації, що використовують фізичні властивості навколишнього середовища.
47. Методи пошуку закладок з використанням металошукачів.
48. Види спеціальних перевірок виділених приміщень.
49. Державне ліцензування діяльності в області захисту інформації.
50. Сертифікація засобів захисту інформації. Основні поняття.
51. Атестування об'єктів інформатизації. Основні поняття.
52. Основні рекомендації щодо захисту інформації від витоку технічними каналами на об'єктах ТЗПІ при розробці технічного проекту
53. Етапи розробки проекту комплексу засобів захисту інформаційно-комунікаційної системи.
54. Принципи адаптації можливостей комплексу засобів захисту до вимог стандартів.
55. Вимоги нормативних документів щодо створення КСЗІ в ІТС
56. Етапи побудови комплексної системи захисту інформації
57. Комплексні системи захисту інформації: призначення, принципи, стратегії
58. Середовища функціонування ІТС. Вміст передпроєктних робіт щодо створення КСЗІ. Порядок розробки і вміст нормативно-розпорядчої документації передпроєктної стадії робіт.
59. Порядок розробки і вміст документів ескізного проекту, робочого та технічного проекту КСЗІ
60. Порядок створення комплексу технічного захисту інформації в ІТС.
61. Принципи розробки та методики випробувань КСЗІ.
62. Практика введення в дію КСЗІ.
63. Види експертизи та її проведення на реальних об'єктах.
64. Процедура впровадження КСЗІ.
65. Супровід КСЗІ в ІТС
66. Складання програм випробувань КСЗІ та розробка методик проведення випробувань.
67. Методи оцінки захищеності інформаційно-комунікаційних систем

МЕТОДИЧНЕ ЗАБЕЗПЕЧЕННЯ

Навчальний процес з дисципліни „Комплексні системи захисту інформації: проєктування, впровадження, супровід” повністю і в достатній кількості забезпечений необхідною навчально-методичною літературою, розміщеною в електронному варіанті в модульному середовищі.

РЕКОМЕНДОВАНА ЛІТЕРАТУРА

Основна

1. Технічні канали витоку інформації. Порядок створення комплексів технічного захисту інформації. Навчальний посібник / Іванченко С.О., Гавриленко О.В., Липський О.А., Шевцов А.С. – К.: ІСЗЗІ НТУУ «КПІ», 2016. - 104 с.
2. Ластівка Г. І. Технічний захист інформації в інформаційних та телекомунікаційних системах: Навчальний посібник / Г. І. Ластівка, П. М. Шпатар - Чернівці: Чернівецький національний університет, 2018. - 252 с
3. Інформаційна безпека: навчальний посібник / [Ю. Я. Бобало, І. В. Горбатий, М. Д. Кіселичник, А. П. Бондарєв та ін.]; за заг. ред. д-ра техн. наук, проф. Ю. Я. Бобала та д-ра техн. наук, доц. І. В. Горбатого. – Львів: Видавництво Львівської політехніки, 2019. – 580 с.
4. Методи і алгоритми захисту інформаційних ресурсів комп'ютерних систем: навчальний посібник / В. М. Джулій, Ю. П. Кльоц, І. В. Муляр, В. М. Чешун. – Хмельницький: ХмНУ, 2020. – 196 с.
5. Cyber Security for Cyber Physical Systems / Saqib Ali, Taiseera Al Balushi, Zia Nadir, Omar Khadeer Hussain. – Cham, Switzerland : Springer, 2018. – 174 p.
6. Інформаційна безпека держави: навчальний посібник/ В.І. Гур’єв, Д.Б. Мехед, Ю.М. Ткач, І.В. Фірсова. – Ніжин: ФОП Лук’яненко В.В. ТПК «Орхідея», 2018. – 166 с.
7. Fundamentals of InformationSystems Security / Editors : David Kim, Michael G. Solomon. – Burlington, Massachusetts : Jones & Bartlett Learning, 2018. – 548 p.
8. Securing the Perimeter: Deploying Identity and Access Management with Free Open Source Software Level / Editors : Michael Schwartz, Maciej Machulak. – Apress, 2018. – 377 p.
9. Security and Privacy inInternet of Things (IoTs): Models, Algorithms, and Implementations / Edited by Fei Hu**. –** Taylor & Francis Group, 2016**. –** 564 p.
10. Cyber-Physical Security: Protecting Critical Infrastructure at the State and Local Level / Editors : Robert M. Clark, Simon Hakim. – Cham, Switzerland : Springer, 2016. – 360 p.
11. Гребенніков В.В. Комплексні системи захисту інформації: проєктування, впровадження, супровід. / В.В. Гребенніков – Ужгород: Ужгородський національний університет, 2013. – 161 с.

Додаткова

12. Practical Information Security Management: A Complete Guide to Planning and Implementation/ Tony Campbell. – Australia: Burns Beach, 2016. – 253 p.
13. Cyber-Development, Cyber-Democracy and Cyber-Defense: Challenges, Opportunities and Implications for Theory, Policy and Practice / Elias G. Carayannis, David F. J. Campbell, Marios Panagiotis Efthymiopoulos. – New York : Springer, 2014. – 360 p.
14. Yevseiev S. The development of the method of multifactor authentication based on hybrid crypto-code constructions on defective codes / S. Yevseiev, H. Kots, S. Minukhin, O. Korol, A. Kholodkova // Восточно-Европейский журнал передовых технологий. – 2017. – № 5(9). – С. 19-35
15. НД ТЗІ 3.7-001-99. Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі. – Чинний від 28 квітня 1999 р. – Київ : ДСТСЗІ СБ, 1999. – [35] с.
16. НД ТЗІ 3.6-001-2000. Технічний захист інформації. Комп’ютерні системи. Порядок створення, впровадження, супроводження та модернізації засобів технічного захисту інформації від несанкціонованого доступу. – Чинний від 20 грудня 2000 р. – Київ : ДСТСЗІ СБ, 2000. – [8] с.
17. НД ТЗІ 3.7-003 -2005. Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі. – Чинний від 28 листопада 2005 р. – Київ : ДСТСЗІ СБ, 2005. – [22] с.
18. НД ТЗІ 1.1-005-07. Захист інформації на об’єктах інформаційної діяльності. Створення

комплексу технічного захисту інформації. Основні положення. – Чинний від 12 грудня 2007 р. – Київ : ДСТСЗІ СБ, 2007. – [7] с.

19. НД ТЗІ 3.3-001-07 Захист інформації на об’єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Порядок розроблення та впровадження заходів із захисту інформації. – Чинний від 12 грудня 2007 р. – Київ : ДСТСЗІ СБ, 2007. – [9] с.

20. НД ТЗІ 2.7-011-2012. Захист інформації на об’єктах інформаційної діяльності. Методичні вказівки з розробки Методики виявлення закладних пристроїв. – Чинний від 23 липня 2012 р. – Київ : Адміністрація Держспецзв’язку, 2012. – [18] с.

21. НД ТЗІ 2.6-001-11. Порядок проведення робіт з державної експертизи засобів технічного захисту інформації від несанкціонованого доступу та комплексних систем захисту інформації в інформаційно-телекомунікаційних системах. – Чинний від 25 березня 2011 р. – Київ : Адміністрація Державної служби спеціального зв’язку та захисту інформації України, 2011. – [130] с.

22. ДСТУ ISO/IEC 27032:2016 (ISO/IEC 27032:2012, IDT). Інформаційні технології. Методи захисту. Настанови щодо кібербезпеки. – Чинний від 2016-27-12. – Київ : ДП «УкрНДНЦ», 2018. – [50] с.

23. Микитишин А. Г. Комплексна безпека інформаційних мережевих систем: навчальний посібник / А.Г. Микитишин, М.М. Митник, П.Д. Стухляк. .– Тернопіль: ТНТУ, 2016. – 255 с

24.Stephen Sakawa Kibwage. Role-Based Access Control Administration of Security Policies and Policy Conflict Resolution in Distributed Systems / Stephen Sakawa Kibwage. – A Dissertation submitted in partial fulfillment of the requirements for the degree of Doctor of Philosophy in Information Systems Graduate School of Computer and Information Sciences. – Nova Southeastern University, 2015. – 111 p.

25. The Internet of Things: Do-It-Yourself Projects with Arduino, Rasberry Pi, and BeagleBone Black / Edited by Donald Norris. – McGraw-Hill Education, 2015. – 582 p.

26. Інформаційна та кібербезпека: соціотехнічний аспект: підручник/ В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко, С. В. Толюпа; за заг. ред. д-ра техн. наук, професора В. Б. Толубка. – К.: ДУТ, 2015. – 288 с.

27. Safeguarding the Information Systems in an Organization through Different Technologies, Policies, and Actions/ Hend K. Alkahtani. – Computer and Information Science. – Vol. 12, No. 2; 2019. – Published by Canadian Center of Science and Education. – P. 117-125.

28. Information Security Standard: Information Technology Resource Management. Virginia Information Technologies Agency (VITA), 2016. – 183 p.

29. The Development of an Intelligent Complex of Radiation-Technological Control of a Safety Barrier / S. Lienkov, O. Banzak, Y. Husak, I. Muliar, V. Cheshun, E. Lenkov // International Journal of Emerging Trends in Engineering Research. – Volume 8. No. 7, July 2020. – P. 3483–3486.

30. Довбня С. Створення системи технічного захисту інформації з використанням матриць небезпечних факторів, що характеризують технічні канали витоку / Сергій Довбня, Андрій Нікірін, Іван Четверіков // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні : науково-технічний збірник. – 2014. – Вип. 1(27). – С. 14-21.

31.Назарук В. Д. Методичні вказівки до лабораторних робіт із навчальної дисципліни "Організація захисту інформації в комп'ютерних системах" / В. Д. Назарук – Рівне : НУВГП, 2018 – 60 с.

ІНФОРМАЦІЙНІ РЕСУРСИ

1. Модульне середовище для навчання MOODLE. Доступ до ресурсу: https://msn.khmnu.edu.ua/.
2. Електронна бібліотека університету. Доступ до ресурсу: http://library.khmnu.edu.ua/.