Силабус курсу

ТЕХНІЧНІ ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЇ

Ступінь вищої освіти – бакалавр
Рік навчання: 4,
Семестр: 7
Кількість кредитів: 5,
Мова викладання: українська

Керівник курсу

ПІП Сергій Кулина
Контактна інформація sersks@wunu.edu.ua

Опис дисципліни

Курс «Технічні засоби захисту інформації» орієнтований на формування компетентностей та умінь щодо технічного захисту інформації для їх використання в сучасних комп'ютерних системах, а також знаннями щодо проявлення різних технічних каналів витоку інформації, шляхів деструктивного впливу на інформацію та засоби її обробки, застосування різних технічних заходів та засобів, які спрямовані на захист інформації на об'єктах інформаційної діяльності.

Вивчення курсу вимагає цілеспрямованої роботи над вивченням спеціалізованої літератури, активної роботи на лекціях та практичних заняттях, самостійної роботи та виконання індивідуальних завдань. Мета курсу полягає в отриманні студентами необхідних знань щодо проявлення технічних каналів витоку інформації, шляхів деструктивного впливу на інформацію та засоби її обробки, застосування заходів та засобів, спрямованих на технічний захист інформації на об'єктах інформаційної діяльності.

Структура курсу

Години лек/лаб	Тема	Результати навчання	Завдання
2/-	Види, джерела та носії інформації, що підлягають захисту.	Використовувати сучасне програмно апаратне забезпечення інформаційно комунікаційних технологій.	Поточне опитування
2/4	Небезпечні сигнали та їх джерела.	Виявляти небезпечні сигнали технічних засобів. Розуміти основні поняття та виявляти небезпечні сигнали технічних засобів.	Ситуаційне завдання
4/2	Технічна розвідка.	Застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно телекомунікаційних систем.	Поточне опитування
4/4	Концепція і методи технічного захисту інформації.	Володіти навичками застосування методів комплексного захисту, знати основні напрямки інженерно-технічного захисту.	Ситуаційне завдання
2/2	Технічні канали витоку інформації.	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.	Поточне опитування

2/2	Електричні канали витоку інформації.	Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик інформаційно телекомунікаційних систем відповідно до вимог нормативних документів системи технічного захисту інформації.	Ситуаційне завдання
4/4	Радіоелектронні канали витоку інформації.	Знати особливості, структуру та види витоку інформації через радіоелектронні канали. Класифікувати типи перешкод.	Поточне опитування
4/4	Акустичні канали витоку інформації.	Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик ІТС відповідно до вимог нормативних документів системи технічного захисту інформації.	Ситуаційне завдання
4/4	Технічні канали витоку інформації на основі закладних пристроїв.	Проводити атестацію (спираючись на облік та обстеження) режимних територій (зон), приміщень тощо в умовах додержання режиму секретності із фіксуванням результатів у відповідних документах.	Поточне опитування
2/2	Методи та засоби захисту від спостереження та підслуховування.	Розуміти поняття енергетичне приховування, звукоізоляція та звукопоглинання. Знати методи та засоби виявлення випромінювання та не випромінюючих закладних пристроїв.	Ситуаційне завдання
2/2	Засоби запобігання витоку інформації через побічні електромагнітні випромінювання	Забезпечувати неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур. Впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки.	Поточне опитування
4/4	Методи і засоби приховування інформації в каналах зв’язку.	Знати методи приховування мовної інформації в каналах зв’язку, засоби контролю телефонних ліній та перехоплення повідомлень в GSM каналах.	Поточне опитування
4/4	Методи і засоби технічної охорони об’єктів. системи сигналізації та відео спостереження.	Знати складові та властивості систем телевізійного спостереження, засобів телевізійної охорони. Основні характеристики засобів запису та реєстрації зображення.	Ситуаційне завдання

Літературні джерела

1. Аль-Амморі Алі. Елементи теорії надійності та інформаційної безпеки комп’ютеризованих систем: навч. посіб . Київ: Видавництво Ліра-К, 2024. - 282с.
2. Богуш В. М. Технічний захист інформації: Навч. погіб. в 2 ч. Ч. 1: Основи технічного захисту інформації / В. М. Богуш, В. Д. Бровко, О.С.Кобус, В.Д. Козюра. Київ: Видавництво Ліра-К, 2022. - 286с.
3. Богуш В.М. Основи кіберпростору, кібербезпеки та кіберзахисту. Навч. Посіб / Богуш В. М., Богуш В. В., Бровко В. Д., Настрадін В. П.. - К.: Видавництво Ліра-К, 2020. — 554 с.
4. Богуш В.М., Бровко В.Д., Кобус О.С., В.Д. Козюра В.Д. Технічний захист інформації: теоретичні основи та організаційно-технічне забезпечення. Київ: Видавництво Ліра-К, 2022. - 286с.
5. Голев Д.В., Кононович В.Г., Хомич С.В. Методики оцінки інформаційної захищеності телекомунікацій. Навчальний посібник. — Одеса : ОНАЗ ім. О. С. Попова, 2013. 217 с.
6. Гуз А.М. Організація захисту інформації з обмеженим доступом : навчальний посібник. Гуз А.М., Касперський І.П., Ткачук Т.Ю. Київ : НА СБУ, 2018. С. 33–58.

7. Гулак Г.М. Методологія захисту інформації. Аспекти кібербезпеки: підручник / Г.М. Гулак – К.: Видавництво НА СБ України, 2020. – 256 с.
8. Євсеєв С.П. Методологія синтезу моделей інтелектуальних систем управління та безпеки об'єктів критичної інфраструктури. Монографія / С.П. Євсеєв, О.Ю. Заковоротний, О.В. Мілов, Г.А. Кучук, О.А. Галуза, М.В. Коваль, О.В. Войтко, Р.В. Грищук – Харків: Вид. «Новий Світ-2000», 2024. 300 с. (Укр. мов.)
9. Козачок В.А. Політики безпеки. Навчальний посібник для студентів вищих навчальних закладів / Козачок В.А., Гайдур Г.І., Гахов С.О., Хмелевський Р.М., Чумак Н.С. – Київ: ДУТ ННІЗІ, 2020. – 167 с.
10. Лаптєв О.А. Виявлення та блокування засобів негласного отримання інформації на об'єктах інформаційної діяльності: навчальний посібник / О.А. Лаптєв, В.А. Савченко, Г.В. Шуклін. – К.: ДУТ, 2020. – 126 с.
11. 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.
12. Остапов С. Е. Технології захисту інформації: навчальний посібник (2-ге видання, стереотипне) / С. Е. Остапов, С. П. Євсеєв, О.Г. Король. – Львів: «Новий Світ- 2000», 2024 . – 678 с.
13. Полторак В.П. Інформаційна безпека та захист даних в комп'ютерних технологіях і мережах. Навчальний посібник. – Київ : КПІ ім. Ігоря Сікорського, 2020. 78 с.
14. Самойленко О. А. Протидія кіберзлочинам: криміналістичний аспект : навчально-методичний посібник / О. А. Самойленко. - Одеса, 2020. 133 с.
15. Чубенко А. Г.. Володілець інформації; Засоби захисту інформації. Термінологічний словник з питань запобігання та протидії легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму, фінансуванню розповсюдження зброї масового знищення та корупції / А. Г. Чубенко, М. В. Лошицький, Д. М. Павлов, С. С. Бичкова, О. С. Юнін. — Київ : Ваіте, 2018. — С. 175; 273.
16. CCTA Risk Analysis and Management Method [Електронний ресурс] – Режим доступу: https://www.giac.org/paper/gsec/1746/qualitative-risk-analysismanagement-tool-cramm/103133 (дата звернення: 21.01.2022)
17. Jason Andress. Foundations of Information Security: A Straightforward Introduction. No Starch Press,US. 2019. – P. 380.

Політика оцінювання

Політика щодо запізнення та перескладання: Роботи, які здаються із порушенням термінів без поважних причин, оцінюються на нижчу оцінку (-20 балів). Перескладання модулів відбувається із дозволу деканату за наявності поважних причин (наприклад, лікарняний).

Політика щодо академічної доброчесності: Усі письмові роботи перевіряються на наявність плагіату і допускаються до захисту із коректними текстовими запозиченнями не більше 20%. Списування під час контрольних робіт та екзаменів заборонені.

Політика щодо відвідування: Відвідування занять є обов'язковим. За об'єктивних причин (наприклад, хвороба, міжнародне стажування) навчання може відбуватись в он-лайн формі за погодженням із керівником курсу.

Оцінювання

Модуль 1		Модуль 2		Модуль 3	Модуль 4	Модуль 5
10%	10%	10%	10%	5%	15%	40%
Поточне оцінювання	Модульний контроль 1	Поточне оцінювання	Модульний контроль 2	Тренінги	Самостійна робота	Екзамен
Оцінка за даний модуль визначається як середнє арифметичне за захист лабораторних робіт №1-8.	Підсумкове модульне тестування за темами № 1-9.	Оцінка за даний модуль визначається як середнє арифметичне за захист лабораторних робіт № 9-13.	Підсумкове модульне тестування за темами № 10-13.	Визначається як середнє арифметичне з оцінок за завдання тренінгу (не менше двох).	Визначається як оцінка за наскрізне завдання самостійної роботи.	1. Теоретичні питання: 2 Питання по 20 балів. 2. 15 тестів по 4 бали.

Шкала оцінювання

За шкалою ЗУНУ (сума балів за всі види навчальної діяльності в межах модуля)	**За національною шкалою**	**За шкалою ECTS**
90-100	відмінно	**A** (відмінно)
85-89	добре	**B** (дуже добре)
75-84		**C** (добре)
65-74	задовільно	**D** (задовільно)
60-64		**E** (достатньо)
35-59	незадовільно	**FX** (незадовільно з можливістю повторного складання)
1-34		**F** (незадовільно з обов’язковим повторним курсом)