Силабус курсу
КОМПЛЕКСНІ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ

Ступінь вищої освіти – бакалавр
Галузь знань – F Інформаційні технології
Спеціальність - F5 Кібербезпека та захист інформації
Освітньо-професійна програма – «Кібербезпека»
Рік навчання: 4
Семестр: 8
Кількість кредитів: 5
Мова викладання: українська

Керівник курсу

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

Опис дисципліни

Курс **«Комплексні системи захисту інформації»** є незамінною складовою навчального процесу для здобувачів спеціальності Кібербезпека та захист інформації. Його метою є навчання здобувачів освіти принципам проектування, впровадження та адміністрування сучасних систем кібербезпеки на основі синтезу організаційних і технічних заходів щодо забезпечення захисту інформації з обмеженим доступом, основ ведення електронного документообігу в умовах сучасних кіберзагроз та витоку сигналів технічними каналами, забезпечення захисту інформації від несанкціонованого доступу на основі вимог міжнародних стандартів з інформаційної безпеки та державних нормативних документів з технології захисту інформації.

Структура курсу

Години лек/пр	Тема	Результати навчання	Завдання
2/2	Сутність і завдання комплексної системи захисту інформації	Поняття комплексної системи захисту інформації Сутність комплексної системи захисту інформації. Призначення комплексної системи захисту інформації. Принципи побудови комплексної системи захисту інформації. Цілі системного підходу до захисту інформації. Стратегії захисту інформації Розробка політики безпеки підприємства. Основні вимоги, що пред'являються до комплексної системи захисту інформаці	Поточне опитування
2/2	Методологічні основи комплексної системи захисту інформації	Основні поняття теорії захисту інформації. Методологія захисту інформації як теоретичний базис комплексної системи захисту інформації. Основні поняття теорії систем.. Системний аналіз і системний підхід. Основні системні уявлення	Поточне опитування

3/2	Визначення складу інформації, що захищається	Методика визначення складу інформації, що захищається. Класифікація інформації за видами таємниці і ступенями конфіденційності. Визначення об'єктів захисту. Сховища носіїв інформації як об'єкт захисту. Методи оцінки захищеності підприємства.	Поточне опитування
2/3	Джерела, способи і результати дестабілізуючого впливу на інформацію	Оцінка загроз безпеки інформації. Явища, фактори і умови дестабілізуючого впливу на захищає інформацію. Джерела дестабілізуючого впливу на інформацію. Види і способи дестабілізуючого впливу на інформацію з боку людей. Види і способи дестабілізуючого впливу на інформацію з боку технічних засобів, технологічних процесів і природних явищ. Визначення причин, обставин і умов дестабілізуючого впливу на інформацію з боку людей. Причини, обставини і умови дестабілізуючого впливу на інформацію з боку технічних засобів, технологічних процесів і природних явищ.	Поточне опитування
2/2	Канали і методи несанкціонованого доступу до інформації	Методика виявлення каналів несанкціонованого доступу до інформації. Визначення можливих методів несанкціонованого доступу до інформації, що захищається. Ділова розвідка як канал несанкціонованого доступу для отримання інформації. Інформаційний продукт як наслідок реалізації несанкціонованих дій. Модель потенційного порушника	Поточне опитування
3/3	Моделювання процесів комплексної системи захисту інформації.	Поняття моделі об'єкта. Моделювання як інструмент аналізу об'єкта КСЗІ. Значення моделювання процесів КСЗІ. Архітектурне побудова комплексної системи захисту інформації	Поточне опитування
2/2	Технологічна побудова комплексної системи захисту інформації	Технологічне побудова організаційної системи КСЗІ. Структура організаційної системи підприємства. Загальний вміст робіт з проектування КСЗІ. Основні стадії проектування КСЗІ. Фактори, що впливають на вибір складу КСЗІ. Модель системи автоматизованого проектування захисту інформації	Поточне опитування
2/2	Кадрове забезпечення комплексної системи захисту інформації	Кадрова політика підприємства при створенні КСЗІ. Етапи роботи з персоналом. Комплексний захист інформації та персонал. Мотивація. Розробка кодексу корпоративної поведінки	Поточне опитування
3/2	Нормативно-методичне забезпечення КСЗІ	Значення нормативно-методичного забезпечення. Склад нормативно-методичного забезпечення. Порядок розробки і впровадження документів підприємства	Поточне опитування

3/2	Управління комплексною системою захисту інформації	Загальні закони кібернетики. Сутність організації процесів управління КСЗІ. Технологія організаційного управління КСЗІ. Структуризація процесів технології управління. Вимоги до системи управління як об'єкту дослідження. Основи методології прийняття управлінського рішення. Загальні вимоги до прийняття управлінського рішення. Роль психологічної теорії прийняття управлінського рішення	Поточне опитування
3/2	Планування діяльності комплексної системи захисту інформації	Цілі планування діяльності КСЗІ. Принципи планування. Способи планування. Основні положення розроблення плану. Стадії планування. Контроль діяльності.	Поточне опитування
3/2	Управління комплексною системою захисту інформації в умовах надзвичайних ситуацій.	Поняття і основні види надзвичайних ситуацій. Технологія прийняття рішення в умовах надзвичайної ситуації. Фактори, що впливають на прийняття рішення. Забезпечення управління КСЗІ в умовах надзвичайних ситуацій. Підготовка заходів на випадок виникнення надзвичайної ситуації.	Поточне опитування

Рекомендовані джерела інформації

1. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» [Електронний ресурс] / База законодавства України // № 80/94-ВР – Режим доступу: http://zakon4.rada.gov.ua/laws/ show/80
2. Комплекс засобів захисту від НСД в АС класу 1 «Рубіж-РСО» версія 2 [Електронний ресурс] / ТОВ «Технічний захист інформації» // 2019 - Режим доступу: http://tzi.com.ua/rubzh-rso-versya-20.html
3. Комплексні системи захисту інформації: проектування, впровадження, супровід. Збірник лекцій [Електронний ресурс] / Гребенніков В.В. // 2019 - Режим доступу: http://www.cryptohistory.ru/for students/ 03-KSZI
4. Операційна система «OpenBSD, шифр BBOS» [Електронний ресурс] / Кампанія «ATMNIS» // 2012 - Режим доступу: http://www.atmnis.com/files/user files/BBOS overview.pdf
5. Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі. НД ТЗІ 3.7-003-05 [Електронний ресурс] / Нормативна база Держспецзв'язку / 2023 - Режимдоступу : https://cip.gov.ua/ua/news/normativni-dokumenti-sistemi-tzi
6. Закон України "Про національну безпеку (2019)
7. НД ТЗІ 1.6-004-2013 Захист інформації на об'єктах інформаційної діяльності. Положення про категоріювання об'єктів, де циркулює інформація з обмеженим доступом, що становить державну таємницю.
8. Information Security Handbook for Network Beginners. National Center of Incident Readiness and Strategy for Cybersecurity (NISC) ver. 2.11e
9. "Комплексна безпека інформації та захист інформаційних ресурсів" автора Олександра С. Горбачова. Видавництво: Каравела. Рік видання: 2019. с. - 127.
10. Яремчук Ю. Є. Комплексні системи захисту інформації: навч. пос. [Електронний ресурс] / Ю. Є. Яремчук, П. В. Павловський, В. С. Катаєв, В. В. Сінюгін. – Режим доступу: https://web.posibnyky.vntu.edu.ua/fmib/41yaremchuk_kompleksni_systemy_zahystu_informaciyi/index.html 2024.
11. Комплексні системи захисту інформації в інформаційнотелекомунікаційних системах:

Навчальний посібник / В. Д. Козюра, В. О. Хорошко, М. Є. Шелест, Ю. М. Ткач, Я.Ю. Усов. – Ніжин: ФОП Лук'яненко В.В., ТПК «Орхідея», 2019. – 144 с.
12. Patterson D.A., Hennessy J.L. Computer Organization and Design: The Hardware/Software Interface. 2021. - 736 с.

Політика оцінювання

Політика щодо дедлайнів і перескладання. Для виконання усіх видів завдань здобувачами освіти і проведення контрольних заходів встановлюються конкретні терміни. Перескладання модулів проводиться в установленому порядку.

Політика щодо академічної доброчесності. Списування під час проведення контрольних заходів заборонені. Під час контрольного заходу здобувач освіти може користуватися лише дозволеними допоміжними матеріалами або засобами, йому забороняється в будь-якій формі обмінюватися інформацією з іншими учасниками, використовувати, розповсюджувати, збирати варіанти контрольних завдань.

Політика щодо відвідування. За об'єктивних причин (наприклад, карантин, воєнний стан, хвороба, закордонне стажування) навчання може відбуватись в дистанційній формі за погодженням із керівником курсу з дозволу дирекції факультету.

Критерії, форми поточного та підсумкового контролю

Підсумковий бал (за 100 – бальною шкалою) з дисципліни «Комплексні системи захисту інформації» визначається як середньозважена величина, в залежності від питомої ваги кожної складової залікового кредиту %:

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 №1-6.	Підсумкове модульне тестування за темами № 1-4.	Оцінка за даний модуль визначається як середнє арифметичне за захист лабораторних робіт № 7-12.	Підсумкове модульне тестування за темами № 5-7.	Визначається як оцінка за виконання одного із завдань тренінгу.	Визначається як оцінка за виконання наскрізного завдання самостійної роботи.	1. Теоретичні питання: 3 питання по 10 балів. 2. 35 тестів по 2 бали.

Шкала оцінювання

За шкалою Університету	**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)