СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ
«ТЕОРЕТИЧНІ ТА ПРАКТИЧНІ ПРОБЛЕМИ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ»

<table>
<tr><td colspan="3">Лектор курсу</td><td colspan="2">Іванченко Євгенія Вікторівна, доктор технічних наук, професор, директор Навчально-наукового інституту кібербезпеки та захисту інформації</td><td colspan="2">Контактна інформація лектора (e-mail), сторінка курсу в GWE</td><td colspan="3">e-mail: e.ivanchenko@duikt.edu.ua
сторінка курсу в Classroom - https://classroom.google.com/c/NzI0NTgwOTM2Njgy?cjc=z4dzlm6
код доступу - z4dzlm6</td></tr>
<tr><td colspan="3">Галузь знань</td><td colspan="2">12 Інформаційні технології</td><td colspan="2">Рівень вищої освіти</td><td colspan="3">доктор філософії</td></tr>
<tr><td colspan="3">Спеціальність</td><td colspan="2">125 Кібербезпека та захист інформації</td><td colspan="2">Семестр</td><td colspan="3">1, 2</td></tr>
<tr><td colspan="3">Освітня програма</td><td colspan="2">Кібербезпека</td><td colspan="2">Тип дисципліни</td><td colspan="3">Цикл обов’язкових компонент ОНП</td></tr>
<tr><td rowspan="2">Обсяг:</td><td>Кредитів ECTS</td><td>Годин</td><td colspan="5">За видами занять:</td></tr>
<tr><td>4</td><td>120</td><td>Лекцій
18</td><td>Семінарських занять
-</td><td>Практичних занять
36</td><td>Лабораторних занять
-</td><td>Самостійна підготовка
66</td></tr>
<tr><td colspan="8">АНОТАЦІЯ КУРСУ</td></tr>
<tr><td colspan="3">Освітні компоненти, які передують вивченню</td><td colspan="5">Методологія наукових досліджень у кібербезпеці</td></tr>
<tr><td colspan="3">Освітні компоненти для яких є базовою</td><td colspan="5">Сучасні методи управління інформаційною та кібербезпекою.</td></tr>
<tr><td>Мета курсу:</td><td colspan="7">Формування системи теоретичних знань та практичних навичок щодо можливих небезпек і ступеня ризику втрат інформації, а також практичних навичок щодо забезпечення технічного захисту інформації. Засвоєння здобувачами понять про науку з області технічного захисту інформації, відомостей про математичні моделі та методи захисту інформації, розуміння процесу наукової діяльності в області захисту і оволодіння методологічними та методичними основами наукового дослідження в галузі систем захисту інформації.</td></tr>
<tr><td colspan="8">Компетентності відповідно до освітньої програми</td></tr>
<tr><td colspan="3">Soft- skills / Загальні компетентності (ЗК)</td><td colspan="5">Hard-skills / Фахові компетентності (СК)</td></tr>
<tr><td colspan="3"></td><td colspan="5">ФК-1. Інтегративна компетентність – здатність до інтеграції знань, умінь і навичок та їх ефективного використання в умовах швидкої адаптації організацій до вимог зовнішнього середовищ, що забезпечують виконання завдань науково-дослідної, науково-педагогічної, управлінської та інноваційної діяльності в інформаційній та безпековій сфері тощо.
ФК-4. Професійна компетентність – стан теоретичної та практичної підготовленості, що забезпечує ефективність вирішення професійних проблем і типових професійних завдань; стан володіння інформаційними технологіями та технологіями захисту інформації; здатність до удосконалення та впровадження у практику інновацій у сфері інформаційної та кібербезпеки; ступінь використання наукової літератури та інших джерел інформації для реалізації інноваційних технологій; здатність до здійснення ефективного пошуку та структурування інформації, до кваліфікованої роботи з різними IP тощо.
ФК-5. Загальнонаукова компетентність – здатність до накопичення професійних вмінь та навичок (діагностування й інтерпретування ситуацій,</td></tr>
</table>

	планування та здійснення наукових досліджень, викладання у вищому навчальному закладі предметів, що відносяться до галузі інформаційних технологій та захисту інформації); здатність до генерування нових знань з теорії захисту інформації та інформаційної безпеки, з проблем алгоритмізації та програмування процесів в системах кібербезпеки; здатність до застосування нових знань у професійній діяльності (проектній, винахідницькій та раціоналізаторській роботі) тощо. **ФК-6. Політехнічна компетентність** – знання загальних (методологічних, історичних, економічних, ергономічних тощо) питань безпекової сфери, принципів дії і будови основних функціональних органів інформаційних систем; здатність до оволодіння спеціалізованими програмними пакетами, протоколами передачі даних, спеціальною мікропроцесорною технікою, сучасними інформаційними та без пековими технологіями; здатність до застосування різноманітних, професійно профільованих знань і практичних навичок у сфері захисту інформації. **ФК-7. Інженерна компетентність** – здатність до виробничо-технологічної діяльності (розробки та впровадження інноваційних технологій інформаційної безпеки, вибору технології ІБ, устаткування та засобів, використання інформаційних технологій; розробки програм і методик випробувань систем інформаційної та кібербезпеки); здатність до організаційно-управлінської діяльності (організації процесу створення та надання інфокомунікаційних послуг); здатність до удосконалення, модернізації та уніфікації систем, засобів і технологій забезпечення безпеки інформаційних і комунікаційних систем, до обробки та перетворення інформації тощо.
Програмні результати навчання (ПРН)	
ПРН-5. Уміти розробляти логічні схеми, складати план-проспекти та технічні завдання на виконання наукових досліджень. **ПРН-13. Уміти** виявляти і формулювати актуальні наукові проблеми, генерувати та інтегрувати нові ідеї та нові знання у сфері захисту інформації, інформаційної та кібербезпеки, представляти їх в усній та/або письмових формах перед фаховою і нефаховою аудиторією. **ПРН-17. Уміти** підтримувати комплексні системи інформаційної та кібербезпеки в стані, необхідному для вирішення завдань захисту інформації. **ПРН-21. Уміти** аналізувати та розробляти алгоритми, методики, моделі та складні програмні комплекси оцінки характеристик і стану систем інформаційної та кібербезпеки. **ПРН-24. Уміти** здійснювати науково-технічне супроводження заходів з формування і коригування програмних комплексів забезпечення безпеки та захисту інформації на об’єктах інформаційної діяльності. **ПРН-25. Уміти** визначати можливості для підприємницької та громадської діяльності за напрямом захисту інформації, організації й забезпечення інформаційної та кібербезпеки об’єктів інформаційної діяльності. **ПРН-31. Уміти** проводити або керувати проведенням наукових і науково-технічних досліджень з питань захисту інформації, організації й забезпечення інформаційної та кібербезпеки об’єктів інформаційної діяльності. **ПРН-32. Уміти** обґрунтовувати раціональні шляхи щодо захисту інформації на об’єктах інформаційної діяльності та інформації, що циркулює в ІТ системах та мережах.	

ОРГАНІЗАЦІЯ НАВЧАННЯ			
Тема, опис теми	**Вид заняття**	**Оцінювання за тему**	**Форми і методи навчання/питання до самостійної роботи**
Розділ 1. Теоретичні та практичні проблеми захисту інформації			
Тема 1. Моделі та способи захисту інформації в ТЗІ **Знати:** Проблеми захисту інформації в Україні. Коротку історію захисту інформації. Сучасні загрози інформаційній безпеці. Правові проблеми. Нормативно-методичні проблеми. Технічні проблеми. Організаційні проблеми. Проблеми метрології та регламенту в системі ТЗІ. Доктрину інформаційної безпеки України. Затверджено Указом Президента України від 25 лютого 2017 року. № 47/2017 Закон України «Про основні засади забезпечення кібербезпеки України». (Відомості Верховної Ради (ВВР), 2017, № 45, ст.403) Закон України «Про національну безпеку України» від 21 червня 2018 року Національні інтереси України в інформаційній сфері. Актуальні загрози національним інтересам та національній безпеці України в інформаційній сфері. Пріоритети державної політики в інформаційній сфері. **Вміти:** обгрунтовувати та реалізовувати системи захисту інформаційних ресурсів з обмеженим доступом на об'єктах інформаційної діяльності, здійснювати вибір методів і засобів захисту інформації з обмеженим доступом на обєктах інформаційної діяльності, здійснювати оцінку систем захисту інформації автоматизованої системи своєму призначенню відповідно до вимог діючих стандартів та нормативних документів, володіти вмінням формувати технології розроблення комплексів захисту інформації з обмеженим доступом та охорони обєктів інформаційної діяльності, розробляти проекти комплексів засобів захисту та охорони обєктів інформаційної діяльності. **Формування компетентностей:** ФК-1, ФК-5. **Результати навчання:** ПРН-13, ПРН-25. **Рекомендовані джерела:** 2, 3, 5, 6, 12, 13, 18.	Лекція 1. 2 години		Лекція-візуалізація
	Практичне заняття 1 2 години	2 бали	Загальні положення. Мета та принципи Доктрини. Національні інтереси України в інформаційній сфері. Актуальні загрози національним інтересам та національній безпеці України в інформаційній сфері. Пріоритети державної політики в інформаційній сфері. Механізм реалізації Доктрини. Прикінцеві положення. Закон «Про основні засади забезпечення кібербезпеки України». визначає правові та організаційні основи забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України у кіберпросторі, основні цілі, напрями та принципи державної політики у сфері кібербезпеки, повноваження державних органів, підприємств, установ, організацій, осіб та громадян у цій сфері, основні засади координації їхньої діяльності із забезпечення кібербезпеки. Закон України «Про національну безпеку України» визначає основи та принципи національної безпеки і оборони, цілі та основні засади державної політики, що гарантуватимуть суспільству і кожному громадянину захист від загроз. Як вказується, цим Законом запроваджується всеосяжний підхід до планування у сферах національної безпеки і оборони.
Тема 1. Моделі та способи захисту інформації в ТЗІ**.**	Самостійна робота 4 години	2 бали	Історичні етапи науки про захист інформації. Доктрина національної безпеки України в інформаційній сфері. Закон України «Про національну безпеку України». Закон «Про основні засади забезпечення кібербезпеки України»
Тема 2. Витоки акустичним, електромагнітним, радіоканалами. Побічні електромагнітні випромінювання. **Знати:** фізичні основи. Середовища поширення сигналів. Розуміти роль фізичних процесів у появі каналів витоку інформації, знати їх класифікацію та характеристики; знати і вміти застосовувати основні	Лекція 2. 2 години		Лекція-візуалізація
	Практичне заняття 2. 2 години	2 бали	Запис звуку, підслуховування і прослуховування; акустоелектричні канали отримання інформації через звукові хвилі з подальшою передачею її через мережі

методи, алгоритми і технічні засоби захисту інформації; Акустичні та віброакустичні канали витоку інформації, електромагнітні, радіоканали, візуальні методи, фотографування, відеозйомка, спостереження. Побічні електромагнітні випромінювання та боротьбу з ними. **Вміти:** виявляти методи та засоби несанкціонованого доступу до інформації та її руйнування; використовувати підходи до формування моделі загроз; підходи до формування моделі порушника та моделі опису цінності інформації: базові поняття; адитивна модель цінності інформації; порядкова шкала цінностей; модель решітки цінностей; MLS решітка; підходи та моделі оцінки збитків автоматизованої системи та ризику її функціонування; обгрунтовувати та реалізовувати системи захисту інформаційних ресурсів з обмеженим доступом на об'єктах інформаційної діяльності на основі правових, організаційних інженерно-технічних заходів до засобів захисту; вміти застосовувати отримані теоретичні знання на практиці при розробленні та впровадженні інформаційнокомунікаційних систем та систем технічного захисту інформації; **Формування компетентностей:** ФК-1, ФК-4, ФК-5, ФК-7. **Результати навчання:** ПРН-13, ПРН-17, ПРН-24, ПРН-25. **Рекомендовані джерела:** 1,4,7,8,11,13,16. 2,3,5,6,12,17,18.			електроживлення; віброакустичні - сигнали, що виникають за допомогою перетворення інформативного акустичного сигналу при впливі його на будівельні конструкції і інженерно-технічні комунікації приміщень, які захищаються; оптичні. електромагнітні - копіювання полів шляхом зняття індуктивних наводок; радіовипромінювання або електричні сигнали від впроваджених в технічні засоби і приміщення спеціальних електронних пристроїв знімання мовної інформації «закладних пристроїв», які модульовані інформативним сигналом
Тема 2. Витоки акустичним, електромагнітним, радіоканалами. Побічні електромагнітні випромінювання.	Самостійна робота 4 години	2 бали	Реалізація системи захисту інформаційних ресурсів з обмеженим доступом на об'єктах інформаційної діяльності, здійснення вибору методів і засобів захисту інформації з обмеженим доступом на об'єктах інформаційної діяльності, здійснення оцінки систем захисту інформації автоматизованої системи відповідно до вимог діючих стандартів та нормативних документів.
Тема 3. Сучасні технології перехоплення інформації. Програмні засоби ТЗІ	Лекція 3. 2 години		Лекція-візуалізація
Знати: аналіз та класифікацію сучасних технічних засобів негласного отримання інформації. Загальні відомості про закладні устрої. Класифікація закладних пристроїв. Загальні характеристики закладних пристроїв. Радіозакладні перевипромінювачі ЗНОІ. Радіозакладки. Акустичні закладні пристрої. Програмні засоби засобів перехоплення інформації та пошуку закладних пристроїв **Вміти:** використовувати комплекс нормативно-правової бази, в тому числі основні концепції, які визначають сучасний стан та подальший розвиток національної та, як її складової, інформаційної безпеки України; застосовувати сучасні прилади, що використовують для блокування каналів витоку інформації; виявляти та блокувати канали	Практичне заняття 3. 2 години	2 бали	Класифікація програмних засобів перехоплення інформації. Програмні засоби закладних пристроїв, для знімання акустичної, інформації, та за електромагнітними і радіоканалами. Класифікація програмних засобів пошуку закладних пристроїв. Програмні засоби індикаторів поля, радіочастотомірів і інтерсепторів. Програмні засоби сканерів приймачів і аналізаторів спектру, нелінійних радіолокаторів.

витоку акустичної та каналів витоку електромагнітної інформації; використовувати методики пошуку радіозакладних пристроїв; дотримуватися вимог нормативних документів, що визначають правила обробки інформації з обмеженим доступом засобами обчислювальної техніки; механізми та засоби захисту від шкідливих програмних засобів **Формування компетентностей:** ФК-1, ФК-4, ФК-5, ФК-7. **Результати навчання:** ПРН-13, ПРН-17, ПРН-24, ПРН-25. **Рекомендовані джерела:** 1,9,10,14,15,16.			
Тема 3. Сучасні технології перехоплення інформації. Програмні засоби ТЗІ.	Самостійна робота 5 годин	2 бали	Галузь використання. Нормативні посилання. Класифікація пристроїв негласного отримання інформації. Реалізація системи захисту інформаційних ресурсів з обмеженим доступом на об'єктах інформаційної діяльності, здійснення вибору методів і засобів захисту інформації з обмеженим доступом на об'єктах інформаційної діяльності, здійснення оцінки систем захисту інформації автоматизованої системи відповідно до вимог діючих стандартів та нормативних документів.
Тема 4. Контроль доступу. **Знати:** Загальні положення. Системи та обладнання СКУД. Організацію проведення перевірок стану СКУД та ТЗІ. Права посадових осіб УРТЗІ НПУ, що здійснюють перевірку стану СКУД та ТЗІ. Порядок проведення перевірок стану СКУД та ТЗІ. Кваліфікація порушень СКУД. Висновки перевірок стану СКУД та критерії їх складання. **Вміти:** обгрунтовувати та реалізовувати системи захисту СКУД на об'єктах інформаційної діяльності, здійснювати вибір методів і засобів захисту інформації з обмеженим доступом на обєктах інформаційної діяльності, розробляти проекти комплексів засобів захисту та охорони обєктів інформаційної діяльності. Використовувати положення про державний контроль за станом технічного захисту інформації. Затверджено Наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України 16.05.2007 N 87. Зареєстровано в Міністерстві юстиції України 10 липня 2007 р. за N 785/14052; положення про контроль за станом технічного захисту інформації в органах і підрозділах Національної поліції України. Наказ від 29.02.2016 № 139. Зареєстровано в Міністерстві юстиції України 23 березня 2016 р. за № 431/28561. **Формування компетентностей:** ФК-1, ФК-4, ФК-5, ФК-7. **Результати навчання:** ПРН-13, ПРН-17, ПРН-24, ПРН-25. **Рекомендовані джерела:** 13,14,17.	Лекція 4. 2 години		Лекція-візуалізація
	Практичне заняття 4. 2 години	2 бали	Системи та обладнання СКУД. Обгрунтування та реалізація системи захисту СКУД на об'єктах інформаційної діяльності.

Тема 4. Контроль доступу.	Самостійна робота 5 годин	2 бали	Наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України 16.05.2007 N 87. Зареєстровано в Міністерстві юстиції України 10 липня 2007 р. за N 785/14052; положення про контроль за станом технічного захисту інформації в органах і підрозділах Національної поліції України. Наказ від 29.02.2016 № 139. Зареєстровано в Міністерстві юстиції України 23 березня 2016 р. за № 431/28561.
Тема 5 Організація пошуку засобів негласного отримання інформації та концепції пошуку цифрових засобів. **Знати:** Математичні моделі перетворення безперервних сигналів у цифровий вид. Дискретизація за часом. Обмеження енергетичного спектра по частоті. Удосконалення методу перетворення сигналу. Аналіз існуючих автоматизованих комплексів пошуку засобів негласного отримання інформації та концепції пошуку цифрових засобів. Сучасна тенденція розвитку. Розробка концепції пошуку цифрових засобів негласного отримання інформації **Вміти:** Розробляти методики для локалізації засобів негласного отримання інформації автоматизованими програмними комплексами та застосування методу пасивної радіолокації для локалізації засобів негласного отримання інформації на основі побічного електромагнітного випромінювання. Методики для локалізації засобів негласного отримання інформації автоматизованими програмними комплексами. Застосування методу пасивної радіолокації для локалізації засобів негласного отримання інформації на основі побічного електромагнітного випромінювання. Кластеризацію на основі мультиагентного підходу. Експериментальна перевірка результатів. Проводити комплексних спеціальних перевірок приміщень. Застосовувати методику виконання робіт на підготовчому етапі. Методологія і порядок інструментального пошуку ЗП. Пошук закладних пристроїв з радіочастотним каналом передачі інформації. Сканування радіочастотного діапазону, аналіз радіоелектронної обстановки в приміщенні, виявлення радіовипромінювальних ЗП за допомогою ПАК DigiScan. Пошук пасивних та закладних пристроїв, що використовують низькочастотні магнітні випромінювання і дослідження приміщень на предмет наявності акустичного і віброакустичного каналу витоку інформації. Пошук закладних пристроїв, що використовують низькочастотні магнітні випромінювання. Пошук пасивних закладних пристроїв. Дослідження приміщень на предмет наявності акустичного і віброакустичного каналу витоку інформації	Лекція 5. 2 години		Лекція-візуалізація
	Практичне заняття 5. 2 години	2 бали	Модель нормального функціонування ІС, визначення параметрів оцінки, показники аномальності
	Практичне заняття 6. 2 години	2 бали	Модель нормального функціонування ІС, визначення параметрів оцінки, показники аномальності
	Лекція 6. 2 години		Лекція-візуалізація
	Практичне заняття 7. 2 години	2 бали	Пошук закладних пристроїв, що використовують низькочастотні магнітні випромінювання. Пошук пасивних закладних пристроїв. Дослідження приміщень на предмет наявності акустичного і віброакустичного каналу витоку інформації

Формування компетентностей: ФК-1, ФК-4, ФК-5, ФК-7. **Результати навчання:** ПРН-5, ПРН-13, ПРН-17, ПРН-21, ПРН-24, ПРН25, ПРН-31,ПРН-32. **Рекомендовані джерела:** 13, 14, 16, 17.			
Тема 5. Організація пошуку засобів негласного отримання інформації та концепції пошуку цифрових засобів.	Самостійна робота 12 годин	6 балів	Радіозакладні перевипромінюючі ЗНОІ. Радіозакладки. Акустичні закладні пристрої.
Розділ 2. Теоретичні та практичні проблеми захисту інформації в мережах			
Тема 6. Аналіз уразливості систем захисту інформації з обмеженим доступом. **Знати:** Аналіз моделей захисту інформації в інформаційних мережах держави. Аналіз побудови основних моделей захисту інформації. Стратегія технічного захисту інформації в захищених інформаційно-телекомунікаційних системах. Комплексна узагальнена математична модель захисту інформації в мережах загального користування. Концептуальні моделі захисту інформації для технологій стаціонарного, стільникового, супутникового зв'язку. Концептуальна модель захисту інформації для технологій стаціонарного зв'язку. Концептуальна модель захисту інформації для технологій стільникового зв'язку. Концептуальна модель захисту інформації для технологій супутникового зв'язку. **Вміти:** Застосовувати методологію синтезу та аналізу диференціально-ігрових моделей та методів моделювання процесів кібернападу на державні інформаційні ресурси. Постановка проблеми. Визначення множини станів СІБ. Вибір стратегій КБз. Оптимізація стратегій КБз та оцінювання РЗ. Прогнозування розвитку динаміки процесу КБн. Оптимізація ресурсів КБз та оцінювання РЗ. Блок аналізу ефективності СІб конфіденційність цілісність доступність. Багатоагентне моделювання для дослідження механізмів захисту інформації в мережі Інтернет. Використання заснованого на многоагентних технологіях моделювання процесів забезпечення безпеки Інтернет. Середовище моделювання. Використання міжмережевих екранів. Особливості функціонування міжмережевих екранів. Основні компоненти міжмережевих екранів. Фільтруючі маршрутизатори. Шлюз сеансового рівня. Шлюзи рівня додатків. Підсилена аутентифікація. Адміністрування і система збору статистики. Основні схеми мережевого захисту на базі міжмережевих екранів. Міжмережевий екран – фільтруючий маршрутизатор. Міжмережевий екран на основі двупортового шлюза. Міжмережевий екран на основі екранованого шлюза. Міжмережевий екран – екранована підмережа. Застосування міжмережевих екранів для організації віртуальних корпоративних	Лекція 7. 2 години		Лекція-візуалізація
	Лекція 8. 2 години		Лекція-візуалізація
	Лекція 9. 2 години		Лекція-візуалізація
	Практичне заняття 8. 2 години	2 бали	Особливості функціонування міжмережевих екранів. Основні компоненти міжмережевих екранів. Фільтруючі маршрутизатори. Шлюз сеансового рівня. Шлюзи рівня додатків. Підсилена аутентифікація. Адміністрування і система збору статистики. Основні схеми мережевого захисту на базі міжмережевих екранів. Міжмережевий екран – фільтруючий маршрутизатор. Міжмережевий екран на основі двупортового шлюза. Міжмережевий екран на основі екранованого шлюза. Міжмережевий екран – екранована підмережа. Застосування міжмережевих екранів для організації віртуальних корпоративних мереж. Типові рішення з застосування міжмережевих екранів для захисту інформаційних ресурс.
	Практичне заняття 9. 2 години	2 бали	Основні поняття про мережі Петрі. Захист програм за допомогою мереж Петрі. Злом програм, захищених за допомогою мереж Петрі.
	Практичне заняття 10. 2 години	2 бали	Визначення множини станів СІБ. Вибір стратегій КБз. Оптимізація стратегій КБз та оцінювання РЗ. Прогнозування розвитку динаміки процесу КБн. Оптимізація ресурсів КБз та оцінювання РЗ. Блок аналізу ефективності СІб конфіденційність цілісність доступність
	Практичне заняття 11. 2 години	2 бали	Використання заснованого на многоагентних технологіях моделювання процесів забезпечення безпеки Інтернет. Середовище моделювання

мереж. Типові рішення з застосування міжмережевих екранів для захисту інформаційних ресурс. Захист програм за допомогою мереж Петрі. Основні поняття про мережі Петрі. Захист програм за допомогою мереж Петрі. Злом програм, захищених за допомогою мереж Петрі **Формування компетентностей:** ФК-1, ФК-4, ФК-5,ФК-6, ФК-7. **Результати навчання:** ПРН-5, ПРН-13, ПРН-17, ПРН-21, ПРН-24, ПРН25, ПРН-31, ПРН-32. **Рекомендовані джерела:** 4, 5, 10, 11.			
Тема 6. Аналіз уразливості систем захисту інформації з обмеженим доступом.	Самостійна робота 18 годин	6 балів	Використання міжмережевих екранів. Захист програм за допомогою мереж Петрі. Методологія синтезу та аналізу диференціально-ігрових моделей та методів моделювання процесів кібернападу на державні інформаційні ресурси Багатоагентне моделювання для дослідження механізмів захисту інформації в мережі Інтернет.
Тема 7. Моделі та способи захисту інформації в соціальних мережах. **Знати:** Особливості функціонування Web серверів. Підсистема розмежування доступу. Підсистема антивірусного захисту. Підсистема контролю цілісності. Підсистема виявлення вторгнень. Підсистема аналізу захищеності. Підсистема криптографічного захисту. Підсистема управління засобами захисту Web-порталу. Аналіз математичних моделей захисту інформації у соціальних мережах Огляд комп'ютерних впливів. Аналіз математичних моделей впливів на системи захисту інформації у соціальних мережах. Засоби захисту. Ієрархія захисту баз даних. Метод моделювання нестаціонарних процесів в системах захисту інформації. Аналіз протоколів роботи та протоколів обміну даних пристроїв в мережі Z-Wave , JavaScript API, з метою недопущення втручання в роботу пристроїв захисту інформації. Використання криптографії. **Вміти:** володіти вмінням методу оцінювання захисту інформації в соціальних мережах з урахуванням довіри між користувачами та інтенсивності передачі інформації. Основні параметри довіри. Математична модель захисту інформації при лінійних параметрах зовнішніх впливів. Математична модель захисту інформації від довіри між користувачами при нелінійних параметрах зовнішніх впливів. Визначення фазового портрету системи захисту інформації. Модель зовнішніх впливів. Визначення фазового портрету системи захисту інформації з урахуванням зовнішніх впливів.	Практичне заняття 12. 2 години	2 бали	Особливості функціонування Web серверів. Підсистема розмежування доступу. Підсистема антивірусного захисту. Підсистема контролю цілісності. Підсистема виявлення вторгнень. Підсистема аналізу захищеності. Підсистема криптографічного захисту. Підсистема управління засобами захисту Web-порталу
	Практичне заняття 13. 2 години	2 бали	Концептуальна модель захисту інформації для технологій стаціонарного зв'язку. Концептуальна модель захисту інформації для технологій стільникового зв'язку. Концептуальна модель захисту інформації для технологій супутникового зв'язку.
	Практичне заняття 14. 2 години	2 бали	Огляд комп'ютерних впливів. Аналіз математичних моделей впливів на системи захисту інформації у соціальних мережах.
	Практичне заняття 15. 2 години	2 бали	Методи та засоби захисту інформації в соціальних мережах. Засоби захисту. Ієрархія захисту баз даних. Метод моделювання нестаціонарних процесів в системах захисту інформації. Аналіз протоколів роботи та протоколів обміну даних пристроїв в мережі Z-Wave , JavaScript API, з метою недопущення втручання в роботу пристроїв захисту інформації. Використання криптографії.
	Практичне заняття 16. 2 години	2 бали	Основні параметри довіри. Математична модель захисту інформації при лінійних параметрах зовнішніх впливів.

Формування компетентностей: ФК-1, ФК-4, ФК-5,ФК-6, ФК-7. **Результати навчання:** ПРН-5, ПРН-13, ПРН-17, ПРН-21, ПРН-24, ПРН25, ПРН-31, ПРН-32. **Рекомендовані джерела:** 3, 4.	Практичне заняття 17. 2 години	2 бали	Математична модель захисту інформації при нелінійних параметрах зовнішніх впливів. Визначення фазового портрету системи захисту інформації.
Тема 7. Моделі та способи захисту інформації в соціальних мережах.	Самостійна робота 18 годин	6 балів	Особливості функціонування Web серверів. Аналіз математичних моделей впливів на системи захисту інформації у соціальних мережах. Розробка методу оцінювання захисту інформації в соціальних мережах з урахуванням довіри між користувачами та інтенсивності передачі інформації. Визначення фазового портрету системи захисту інформації з урахуванням зовнішніх впливів.
Іспит	Практичне заняття 18. 2 години	40 балів	Іспит у письмовій формі.

МАТЕРІАЛЬНО-ТЕХНІЧНЕ ЗАБЕЗПЕЧЕННЯ ДИСЦИПЛІНИ

- Мультимедійний проектор;
- Комп‘ютерне обладнання, мережа Інтернет;
- Навчальна лабораторія засобів контролю доступу;
- Навчальна лабораторія технічного захисту інформації «PIAC».

ІНФОРМАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ ДИСЦИПЛІНИ

1. Методи та засоби технічного захисту інформації: Опорний конспект лекцій [Електронний ресурс] : навч. посіб. для студ. спец. 125 «Кібербезпека» / КПІ ім. Ігоря Сікорського ; уклад.: В.М. Луценко, Д.О. Прогонов. – Електронні текстові дані (1 файл: 1,80 Мбайт). – Київ : КПІ ім. Ігоря Сікорського, 2021. – 289 с. https://ela.kpi.ua/bitstreams/1387ecef-b4cb-4554-b55f-7c34e52b3605/download
2. 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. – 286 с. https://knushop.com.ua/image/catalog/lira20230617/pdf/13054.pdf?srsltid=AfmBOoqRT7snkVTSTjDs_hQJh5fcXTcWSrRXLaQCdYffqFs6whQ8pNvF
3. Котенко А.М. Курс лекцій для студентів з галузі знань 12 «Інформаційні технології» за спеціальністю 125 «Кібербезпека та захист інформації» з дисципліни «Системи контролю та управління доступом на ОІД»/ А.М. Котенко. Державний університет інформаційно-комунікаційних технологій,–К., ДУІКТ, 2024. – 79 с. https://duikt.edu.ua/uploads/l_1372_10715986.pdf
4. Ахрамович В.М. Методологічні основи захисту інформації в соціальних мережах. Дисертація на здобуття наукового ступеня доктора технічних наук, спеціальність 05.13.21 «Системи захисту інформації» К.,2021.-302с.
5. Інформаційна безпека. Підручник / В. В. Остроухов, М. М. Присяжнюк, О. І. Фармагей, М. М. Чеховська та ін.; під ред. В. В. Остроухова – К.: Видавництво Ліра-К, 2021. – 412 с. https://lira-k.com.ua/preview/12867.pdf?srsltid=AfmBOoqzg23vDnRFvDb9QAjOhJF4yty_1eKmcfB1cF2H8gWrD-P1F2G5
6. Безпека інформації : конспект лекцій / укладач О. С. Кушнерьов. – Суми : Сумський державний університет, 2021. – 99 с. https://essuir.sumdu.edu.ua/bitstream-download/123456789/85989/3/Kushnerov.pdf;jsessionid=DAF96BD511913EA27F430BDEA0BD267F
7. Інформаційна безпека та кібербезпека держави: навчальний посібник / Н.М. Титова, Н.М. Рідей, В.П. Настрадін, М.М. Присяжнюк, С.М. Мамченко, С.В. Артюх, Р.О. Яворська. // К., Вид-во Ліра-К, 2024, 224 с. https://jurkniga.ua/contents/informatsiyna-bezpeka-ta-kiberbezpeka-derzhavi.pdf?srsltid=AfmBOoonlSD1-wrG2YmF-bHwmhdSCi7OHzlEKVrfRyGvvlfca4VA4Sxx
8. О.І. Чобаль, І.І. Трикур, М.П. Самохвалов, В.М. Різак. Методи і засоби захисту інформації: лабораторний практикум. – Ужгород: ДВНЗ „Ужгородський національний університет”. – 2023. – 80 с.

https://dspace.uzhnu.edu.ua/jspui/bitstream/lib/56222/1/%D0%9F%D0%BE%D1%81%D1%96%D0%B1%D0%BD%D0%B8%D0%BA_%D0%9B%D0%B0%D0%B1_%D1%80%D0%BE%D0%B1_%D0%9C%D0%97%D0%97%D0%86_2023.pdf
9. Програмні технології захисту інформації: конспект лекцій для здобувачів першого (бакалаврського) рівня вищої освіти, спеціальності 121 Інженерія програмного забезпечення факультету інформаційних технологій УжНУ / Укладач: д.т.н., доц. Поліщук В.В. – Ужгород: 2023. – 76 с. https://dspace.uzhnu.edu.ua/jspui/bitstream/lib/19693/3/%D0%9A%D0%BE%D0%BD%D1%81%D0%BF%D0%B5%D0%BA%D1%82%20%D0%BB%D0%B5%D0%BA%D1%86%D1%96%D0%B9%20%D0%9F%D0%A2%D0%97%D0%86.pdf
10. Безпека інфокомунікацій та безперервність бізнес-процесів. Електронний навчальний посібник. / Г.В. Косован, Г.І. Ластівка, П.М. Шпатар. // Чернівці, ЧНУ, 2023. 153 с. https://drive.google.com/file/d/1VKk9f3CLavO5ctgWuc-TXOkZKhR1FQOW/view?pli=1
11. Ліцензування, атестація та сертифікація в сфері безпеки об'єктів інформаційної діяльності. Електронний навчальний посібник / Кушнір М.Я., Горбулик В.І. // Чернівці, ЧНУ, 2023. 104 с. https://drive.google.com/file/d/1SdEY2WkJsDj1C4it7YCCHbn_PPynvWPl/view
12. Засоби радіопротидії в інформаційно-телекомунікаційних системах. Електронний навчальний посібник. / Браїловський В.В., Рождественська М.Г., Гресь О.В., Косован Г.В. // Чернівці, ЧНУ, 2021. 130 с. https://drive.google.com/file/d/1PQBSe2ORgpfeYPGvbLiGYTRNexlcVWg9/view
13. Управління інформаційною безпекою. Навчальний посібник / [уклад.: Толюпа С.В., Політанський Л.Ф., Політанський Р.Л., Лесінський В.В.] Чернівці.: Чернівецький нац. ун-т ім. Ю.Федьковича, 2021. – 540 с. https://drive.google.com/file/d/160LvEO5XQnbtZFsQb2L_wA8bJEnjBnch/view
14. Лаптєв О.А., Савченко В.А., Шуклін Г.В. Виявлення та блокування засобів негласного отримання інформації на об'єктах інформаційної діяльності Навчальній посібник Київ – 2020.-126 с. https://duikt.edu.ua/uploads/l_2031_50136601.pdf
15. Мірошніков В.В., Мілих М.Л., Чумак О.І. Системи передачі цифрової інформації: К.: УНДІЗ, 2021. 82 с.
16. Самохвалов Ю.Я., Темніков В.О., Хорошко В.О. Організаційно-технічне забезпечення захисту інформації / За ред. проф. В.О. Хорошка – К.: Видавництво НАУ, 2020. – 208 с.
17. Іванченко Є.В., Корченко О.Г., Бакалинський О.О., Мялковський Д.В. Зубков Д.А., Метод оцінювання рівня підвищення стану кіберзахисту об'єктів критичної інфраструктури держави // Наукоємні технології.: науковий журнал: НАУ, № 1 (61). 2024. С.3-20. https://jrnl.nau.edu.ua/index.php/SBT/article/view/18509. DOI: https://doi.org/10.18372/2310-5461.61.18509 .
18. Іванченко Є.В., Корченко О.Г. Система оцінювання підвищення стану кіберзахисту об'єктів огляду критичної інфраструктури держави. Безпека інформації. Том 30 № 1 (2024). С. 95-99. https://jrnl.nau.edu.ua/index.php/ Infosecurity/article/view/18610. https://doi.org/10.18372/2225-5036.30.18610 .

ПОЛІТИКА КУРСУ («ПРАВИЛА ГРИ»)

- Курс передбачає роботу в колективі.
- Середовище в аудиторії є дружнім, творчим, відкритим до конструктивної критики.
- Освоєння дисципліни передбачає обов'язкове відвідування лекцій і семінарських занять, а також самостійну роботу.
- Самостійна робота включає в себе теоретичне вивчення питань, що стосуються тем лекційних занять, які не ввійшли в теоретичний курс, або ж були розглянуті коротко, їх поглиблена проробка за рекомендованою літературою.
- Усі завдання, передбачені програмою, мають бути виконані у встановлений термін.
- Якщо здобувач відсутній з поважної причини, він презентує виконані завдання під час самостійної підготовки та консультації викладача.
- Під час роботи над завданнями не допустимо порушення академічної доброчесності: при використанні Інтернет ресурсів та інших джерел інформації здобувач повинен вказати джерело, використане в ході виконання завдання.

КРИТЕРІЇ ТА МЕТОДИ ОЦІНЮВАННЯ

Умовою допуску до підсумкового контролю є набрання здобувачем 60 балів у сукупності за всіма темами дисципліни.

Форми контролю	**Види навчальної роботи**	Оцінювання
ПОТОЧНИЙ КОНТРОЛЬ	• Виконання практичних робіт	34 бали
	• Самостійна робота	26 балів
ПІДСУМКОВЕ	Метою іспиту є контроль сформованості практичних навичок та професійних	40 балів

ОЦІНЮВАННЯ ***Іспит***	компетентностей, необхідних для виконання професійних обов'язків. Іспит проходить у письмовій формі..	

Додаткова оцінка	
Види навчальної роботи	**Оцінювання**
Участь у наукових конференціях, підготовка наукових публікацій за тематикою освітньої компоненти:	
- Тези доповіді на фаховій конференції.	3 бали
- Стаття у фаховому виданні.	5 балів
- Стаття в іноземному рецензованому виданні.	10 балів
Максимальна кількість додаткових балів, які можуть бути зараховані здобувачу освіти - 10 балів.	

ПІДСУМКОВА ОЦІНКА ЗА ДИСЦИПЛІНУ

бали	**Критерії оцінювання**	**Рівень компетентності**	**Оцінка** */запис в екзаменаційній відомості*
90-100	Здобувач демонструє повні й міцні знання навчального матеріалу в обсязі, що відповідає робочій програмі дисципліни, правильно й обґрунтовано приймає необхідні рішення в різних нестандартних ситуаціях. Вміє реалізувати теоретичні положення дисципліни в практичних розрахунках, аналізувати та співставляти дані об'єктів діяльності фахівця на основі набутих з даної та суміжних дисциплін знань та умінь. Знає сучасні технології та методи розрахунків з даної дисципліни. За час навчання при проведенні практичних занять, при виконанні індивідуальних/контрольних завдань проявив вміння самостійно вирішувати поставлені завдання, активно включатись в дискусії, може відстоювати власну позицію в питаннях та рішеннях, що розглядаються. Зменшення 100-бальної оцінки може бути пов'язане з недостатнім розкриттям питань, що стосується дисципліни, яка вивчається, але виходить за рамки об'єму матеріалу, передбаченого робочою програмою, або Здобувач проявляє невпевненість в тлумаченні теоретичних положень чи складних практичних завдань.	**Високий** Повністю забезпечує вимоги до знань, умінь і навичок, що викладені в робочій програмі дисципліни. Власні пропозиції здобувача в оцінках і вирішенні практичних задач підвищує його вміння використовувати знання, які він отримав при вивчені інших дисциплін, а також знання, набуті при самостійному поглибленому вивчені питань, що відносяться до дисципліни, яка вивчається.	Відмінно / Зараховано (A)
82-89	Здобувач демонструє гарні знання, добре володіє матеріалом, що відповідає робочій програмі дисципліни, робить на їх основі аналіз можливих ситуацій та вміє застосовувати теоретичні положення при вирішенні практичних задач, але допускає окремі неточності. Вміє самостійно виправляти допущені помилки, кількість яких є незначною. Знає сучасні технології та методи розрахунків з даної дисципліни. За час навчання при проведенні практичних занять, при виконанні індивідуальних / контрольних завдань та поясненні прийнятих рішень, дає вичерпні пояснення.	**Достатній** Забезпечує здобувачу самостійне вирішення основних практичних задач в умовах, коли вихідні дані в них змінюються порівняно з прикладами, що розглянуті при вивчені дисципліни.	Добре / Зараховано (B)
75-81	Здобувач в загальному добре володіє матеріалом, знає основні положення матеріалу, що відповідає робочій програмі дисципліни, робить на їх основі аналіз можливих ситуацій та вміє застосовувати при вирішенні типових практичних завдань, але допускає окремі неточності. Вміє пояснити основні положення	**Достатній** Конкретний рівень, за вивченим матеріалом робочої програми дисципліни.	Добре / Зараховано (C)

	виконаних завдань та дати правильні відповіді при зміні результату при заданій зміні вихідних параметрів. Помилки у відповідях/ рішеннях/ розрахунках не є системними. Знає характеристики основних положень, що мають визначальне значення при проведенні практичних занять, при виконанні індивідуальних / контрольних завдань та поясненні прийнятих рішень, в межах дисципліни, що вивчається.	Додаткові питання про можливість використання теоретичних положень для практичного використання викликають утруднення.	
67-74	Здобувач засвоїв основний теоретичний матеріал, передбачений робочою програмою дисципліни, та розуміє постанову стандартних практичних завдань, має пропозиції щодо напрямку їх вирішень. Розуміє основні положення, що є визначальними в курсі, може вирішувати подібні завдання тим, що розглядались з викладачем, але допускає значну кількість неточностей і грубих помилок, які може усувати за допомогою викладача. .	**Середній** Забезпечує достатньо надійний рівень відтворення основних положень дисципліни.	Задовільно / Зараховано (D)
60-66	Здобувач має певні знання, передбачені в робочій програмі дисципліни, володіє основними положеннями, що вивчаються на рівні, який визначається як мінімально допустимий. З використанням основних теоретичних положень, здобувач з труднощами пояснює правила вирішення практичних/розрахункових завдань дисципліни. Виконання практичних / індивідуальних / контрольних завдань значно формалізовано: є відповідність алгоритму, але відсутнє глибоке розуміння роботи та взаємозв'язків з іншими дисциплінами.	**Середній** Є мінімально допустимим у всіх складових навчальної програми з дисципліни.	Задовільно / Зараховано (E)
35-59	Здобувач може відтворити окремі фрагменти з курсу. Незважаючи на те, що програму навчальної дисципліни здобувач виконав, працював він пасивно, його відповіді під час практичних робіт в більшості є невірними, необґрунтованими. Цілісність розуміння матеріалу з дисципліни у здобувача відсутні.	**Низький** Не забезпечує практичної реалізації задач, що формуються при вивчені дисципліни.	Незадовільно з можливістю повторного складання) / Не зараховано (FX) *В залікову книжку не проставляється*
0-34	Здобувач повністю не виконав вимог робочої програми навчальної дисципліни. Його знання на підсумкових етапах навчання є фрагментарними. Здобувач не допущений до здачі екзамену/заліку.	**Незадовільний** Здобувач не підготовлений до самостійного вирішення задач, які окреслює мета та завдання дисципліни.	Незадовільно з обов'язковим повторним вивченням / Не допущений (F) *В залікову книжку не проставляється*

ПОЛІТИКА ДОБРОЧЕСНОСТІ

Здобувач вищої освіти виконуючи самостійну або індивідуальну роботу повинен дотримуватись політики доброчесності. У разі наявності плагіату в будь-яких видах робіт здобувача, він отримує незадовільну оцінку і повинен повторно виконати завдання, які передбачені у Силабусі.