ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет інформаційних технологій
Кафедра кібербезпеки

ЗАТВЕРДЖУЮ
Декан ФІТ
_____ Тетяна ГОВОРУЩЕНКО
«_31_» _____08_____ 2024 р.

СИЛАБУС

Навчальна дисципліна: "*Моніторинг та менеджмент інформаційної безпеки*"

Освітньо-професійна програма: «Кібербезпека та захист інформації»

Рівень вищої освіти: другий (магістерський)

Загальна інформація

Позиція	Інформація
Викладач(і)	Тітова Віра Юріївна
Профайл викладач(ів)	https://kb.khmnu.edu.ua/sklad-kafedry/
E-mail викладача(ів)	v.titova231@gmail.com
Контактний телефон	Наявний в ІСУ
Сторінка дисципліни в ІСУ	https://msn.khnu.km.ua/course/view.php?id=7526
Сторінки інтернет-ресурсів для онлайн занять	ZOOM: https://us05web.zoom.us/j/521227760 * пароль у викладача, старости групи і на сторінці дисципліни в ІСУ
Навчальний рік, семестр	2024-2025, семестр I (осінньо-зимовий) 2024-2025, семестр II (зимово-весняний)
Консультації	Очні: згідно графіку консультацій Онлайн: за необхідністю та попередньою домовленістю

Характеристика дисципліни

Форма навчання	Курс	Семестр	Обсяг дисципліни		Кількість годин						Курсовий проект	Курсова робота	Форма семестрового контролю	
					Аудиторні заняття				Індивідуальна робота студента	Самостійна робота, у т.ч. ІРС				
			Кредити ЄКТС	Години	Разом	Лекції	Лабораторні роботи	Практичні заняття					Залік	Іспит
ОД	1	1	5	150	51	17	34	-	-	99	-	-	-	+
ОД	1	2	4	120	54	18	36	-	-	66	-	-	-	+
Разом:			**9**	**270**	**105**	**35**	**70**	**-**	**-**	**165**	**-**	**-**	**-**	**2**

Анотація дисципліни

Дисципліна викладається для студентів денної форми навчання спеціальності «Кібербезпека та захист інформації». При викладанні дисципліни використовуються наступні форми (методи) навчання: словесні та наочні (лекції); практичні та частково-пошукові (лабораторні роботи); пояснювально-ілюстративні та дослідницькі (самостійна робота).

Пререквізити – вихідна (1 семестр), методологія організації атак та тестування на проникнення (2 семестр)

Кореквізити – професійна практика.

Мета і завдання дисципліни

Метою викладання навчальної дисципліни є формування у майбутніх спеціалістів умінь та компетенцій для забезпечення аудиту, моніторингу та менеджменту інформаційної безпеки у комп'ютерних та інформаційно-комунікаційних системах; розвиток у студентів фахового стилю мислення; надання глибоких та міцних знань з питань управління інцидентами та ризиками інформаційної та/або кібербезпеки в умовах широкого використання сучасних інформаційних технологій.

Предметом дисципліни є сучасні процеси дослідження, аналізу, створення та забезпечення функціонування інформаційних систем і технологій, інших бізнес-операційних процесів на об'єктах інформаційної діяльності та критичних інфраструктур сфери інформаційної безпеки та/або кібербезпеки; інформаційні ресурси різних класів (в т.ч. державні інформаційні ресурси); програмне та програмно-апаратне забезпечення (засоби) кіберзахисту; системи управління інформаційною безпекою та/або кібербезпекою; технології, методи, моделі та засоби інформаційної безпеки та/або кібербезпеки; системи та комплекси створення, обробки, передачі, зберігання, знищення, захисту та відображення даних (інформаційних потоків).

Завданням дисципліни є забезпечити набуття компетентностей та досягнення програмних результатів навчання відповідно до освітньо-професійної програми підготовки магістрів зі спеціальності «Кібербезпека та захист інформації»:

***компетентності*:**

КЗ4. Здатність оцінювати та забезпечувати якість виконуваних робіт.

КФ4. Здатність аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації, формувати стратегію і політики інформаційної безпеки з урахуванням вітчизняних і міжнародних стандартів та вимог.

КФ5. Здатність до дослідження, системного аналізу та забезпечення безперервності бізнес/операційних процесів з метою визначення вразливостей інформаційних систем та ресурсів, аналізу ризиків та визначення оцінки їх впливу у відповідності до встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.

КФ7. Здатність досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому.

КФ9. Здатність аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес/операційних процесів в галузі інформаційної безпеки та/або кібербезпеки організації в цілому.

КФ10. Здатність провадити науково-педагогічну діяльність, планувати навчання, контролювати і супроводжувати роботу з персоналом, а також приймати ефективні рішення з питань інформаційної безпеки та/або кібербезпеки.

КФ11. Здатність проводити сканування на вразливості і розпізнавати вразливості в системах безпеки інформації, застосовувати методи виявлення вторгнень на базі хоста та мережі за допомогою технологій виявлення вторгнень, інтерпретувати інформацію, зібрану інструментами моніторингу мережі, аналізувати шкідливе програмне забезпечення.

результати навчання:

РН4. Застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки.

РН6. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення.

РН9. Аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації на базі стратегії і політики інформаційної безпеки.
РН10. Забезпечувати безперервність бізнес/операційних процесів, а також виявляти уразливості інформаційних систем та ресурсів, аналізувати та оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації.
РН12. Досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому.
РН14. Аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес\операційних процесів у сфері інформаційної та\або кібербезпеки в цілому.
РН16. Приймати обґрунтовані рішення з організаційно-технічних питань інформаційної безпеки та/або кібербезпеки у складних і непередбачуваних умовах, у тому числі із застосуванням сучасних методів та засобів оптимізації, прогнозування та прийняття рішень.
РН18. Планувати навчання, а також супроводжувати та контролювати роботу з персоналом у напряму інформаційної безпеки та/або кібербезпеки.
РН21. Використовувати методи натурного, фізичного і комп'ютерного моделювання для дослідження процесів, які стосуються інформаційної безпеки та/або кібербезпеки.
РН24. Розпізнавати та класифікувати типи вразливостей і пов'язаних з ними атак, виявляти вторгнення на базі хоста та мережі за допомогою технологій виявлення вторгнень, використовувати аналізатори протоколів та виконувати аналіз трафіку на рівні пакетів, перевіряти попередження системи виявлення вторгнень щодо мережного трафіку за допомогою інструментів аналізу пакетів для локалізації та видалення шкідливого програмного забезпечення.
РН25. Характеризувати та аналізувати мережний трафік для виявлення аномальної активності (метадані), шкідливих дій, потенційних загроз мережним ресурсам, слабких місць, методів експлуатації, впливу на систему та інформацію.

Студент, який успішно завершив вивчення дисципліни, повинен: *застосовувати*, *інтегрувати*, *розробляти*, *впроваджувати* та *удосконалювати* сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки; *аналізувати* та *оцінювати* захищеність систем, комплексів та засобів кіберзахисту; *аналізувати*, *розробляти* і *супроводжувати* систему управління інформаційною безпекою організації; *забезпечувати* безперервність бізнес/операційних процесів, а також *аналізувати* та *оцінювати* ризики для інформаційної безпеки організації; *досліджувати, розробляти* та *впроваджувати* методи і заходи протидії кіберінцидентам, *здійснювати* процедури управління, контролю та розслідування, а також *надавати* рекомендації щодо попередження та аналізу кіберінцидентів в цілому; *аналізувати*, *розробляти* і *супроводжувати* систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій; *приймати* обґрунтовані рішення з організаційно-технічних питань інформаційної безпеки та/або кібербезпеки у складних і непередбачуваних умовах, у тому числі із застосуванням сучасних методів та засобів оптимізації, прогнозування та прийняття рішень; *планувати* навчання, а також *супроводжувати* та контролювати роботу з персоналом у напряму соціотехнічної безпеки; *використовувати* методи комп'ютерного моделювання для дослідження процесів, які стосуються інформаційної безпеки та/або кібербезпеки; *виявляти* вторгнення на базі хоста та мережі за допомогою технологій виявлення вторгнень, *використовувати* аналізатори протоколів та *виконувати* аналіз трафіку на рівні пакетів, *перевіряти* попередження системи виявлення вторгнень щодо мережного трафіку за допомогою інструментів аналізу пакетів для локалізації та видалення шкідливого програмного забезпечення; *характеризувати* та *аналізувати* мережний трафік для виявлення аномальної активності (метадані), шкідливих дій, потенційних загроз мережним ресурсам.

Тематичний і календарний план вивчення дисципліни (1 семестр)

№ тижня	Тема лекції*	Тема лаб. роботи **	Самостійна роботи		
			Зміст	Год.	Література
1	**Тема 1. Моніторинг інформаційної безпеки** Методології та прийоми виявлення атак/вторгнень	**ЛР1**. Налаштування мережного середовища для моніторингу інформаційної безпеки	Опрацювання теоретичного матеріалу лекції №1.	5	[1] с. 34-42 [2] с. 154-205 [5] с. 62-112 [37] [38] [39]
2	-	**ЛР1.** Підгрупа 2.	Підготовка до виконання лабораторної роботи №1	6	[1], с. 9-23
3	**Тема 1. Моніторинг інформаційної безпеки** Особливості організації моніторингу інформаційно-комунікаційних систем та їх компонентів	**ЛР2.** Моніторинг зараження ARP-кешу	Опрацювання теоретичного матеріалу лекції №2.	5	[2] с. 205-231 [3] [4] с. 70-80 [5] с. 39-62
4	-	**ЛР2.** Підгрупа 2.	Підготовка до захисту лабораторної роботи №1. Підготовка до виконання лабораторної роботи №2.	6	[1], с. 9-23
5	**Тема 1. Моніторинг інформаційної безпеки** Особливості розробки та супроводу системи моніторингу на об'єктах інформаційної діяльності	**ЛР3.** Моніторинг та аналіз мережного трафіку (системи Snort та Suricata)	Опрацювання теоретичного матеріалу лекції №3.	5	[2] с. 205-231 [3] [5] с. 112-165 [32]
6	-	**ЛР3.** Підгрупа 2.	Підготовка до захисту лабораторної роботи №2. Підготовка до виконання лабораторної роботи №3.	6	[1], с. 9-23 [5] с. 103-112 [43]
7	**Тема 1. Моніторинг інформаційної безпеки** Аутсорсинг інформаційної безпеки, як інструмент моніторингу	**ЛР4.** Моніторинг та аналіз процесів операційних систем Linux та Windows	Опрацювання теоретичного матеріалу лекції №4.	5	[6] с. 137-164, 203-226 [7] с. 76-82 [33] [34]
8	-	**ЛР4.** Підгрупа 2.	Підготовка до захисту лабораторної роботи №3. Підготовка до виконання лабораторної роботи №4.	6	[5] с. 73-82, 103-112, 142-148 [43]

9	**Тема 2. Тактики, прийоми і процедури протидії кіберінцидентам** Аналіз кіберінцидентів	**ЛР5.** Налаштування віртуалізації на рівні ОС для створення ізольованих програмних середовищ (побудова контейнерів).	Опрацювання теоретичного матеріалу лекції №5.	5	[8] с. 116-122 [11] [12] с. 116-151 [40] [41]
10	-	**ЛР5.** Підгрупа 2.	Підготовка до захисту лабораторної роботи №4. Підготовка до виконання лабораторної роботи №5.	6	[5] с. 73-82, 139-148
11	**Тема2. Тактики, прийоми і процедури протидії кіберінцидентам** Методологія реагування на інциденти та їх обробки	**ЛР6.** Моніторинг та аналіз шкідливого програмного забезпечення	Опрацювання теоретичного матеріалу лекції №6.	5	[9] [12] с. 151-188 [42]
12	-	**ЛР6.** Підгрупа 2.	Підготовка до захисту лабораторної роботи №5. Підготовка до виконання лабораторної роботи №6.	6	[5] с. 139-142 [16] с. 25-34, 68-85
13	**Тема 2. Тактики, прийоми і процедури протидії кіберінцидентам** Соціотехнічна безпека	**ЛР7.** Проєктування та впровадження системи моніторингу та реагування на інциденти на основі платформи MISP	Опрацювання теоретичного матеріалу лекції №7.	6	[10] с. 69-268
14	-	**ЛР7.** Підгрупа 2.	Підготовка до захисту лабораторної роботи №6. Підготовка до виконання лабораторної роботи №7.	6	[15] [16] с. 25-34, 68-85
15	**Тема 2. Тактики, прийоми і процедури протидії кіберінцидентам** Планування безперервності роботи	**ЛР8.** Дослідження подій та інцидентів, ведення журналів реєстрації, реагування на інциденти	Опрацювання теоретичного матеріалу лекції №8.	6	[8] с. 122-128 [14] с. 239-250
16	-	**ЛР8.** Підгрупа 2.	Підготовка до захисту лабораторної роботи №7. Підготовка до виконання лабораторної роботи №8.	6	[12] с. 170-188 [15]

17	**Тема 2. Тактики, прийоми і процедури протидії кіберінцидентам** Аналіз розвідувальних даних щодо кіберзагроз та кіберінцидентів (CTI)	Підсумкове заняття **Контрольна робота**	Опрацювання теоретичного матеріалу лекції №9. Підготовка до захисту лабораторної роботи №8. Підготовка до контрольної роботи за пройденим матеріалом.	8	[12] с. 170-188 [13] с. 59-119, 220-279

*** лекції проводяться по 2 години раз на два тижні;**
**** лабораторні проводяться по 4 години раз в два тижні.**

Тематичний і календарний план вивчення дисципліни (2 семестр)

№ тижня	Тема лекції*	Тема лаб. роботи **	Самостійна роботи		
			Зміст	Год.	Література
1	**Тема 1. Моделювання та оцінювання безпеки систем** Моделювання об'єктів і систем захисту	**ЛР1**. Дослідження моделей безпечної одношляхової маршрутизації з метрикою протоколу RIP	Опрацювання теоретичного матеріалу лекції №1.	3	[24] с. 240-298, 386-402 [26] с. 482-545 [27] с. 30-37 [28] с. 34-169, 283-319 [54]
2	-	**ЛР1.** Підгрупа 2.	Підготовка до виконання лабораторної роботи №1	4	[29] с. 42-63 [31] с. 195-214
3	**Тема 1. Моделювання та оцінювання безпеки систем** Сучасні підходи в моделюванні систем і засобів кіберзахисту	**ЛР2.** Дослідження моделей безпечної багатошляхової маршрутизації з метрикою протоколу IGRP. Балансування навантаження за технологією Traffic Engineering	Опрацювання теоретичного матеріалу лекції №2.	3	[24] с. 465-490 [30] с. 9-66 [47] [48] [49]
4	-	**ЛР2.** Підгрупа 2.	Підготовка до захисту лабораторної роботи №1. Підготовка до виконання лабораторної роботи №2.	4	[29] с. 42-63 [31] с. 195-214
5	**Тема 1. Моделювання та оцінювання безпеки систем** Задачі і методи оцінювання безпеки систем	**ЛР3.** Дослідження моделей безпечної маршрутизації фрагментованих повідомлень	Опрацювання теоретичного матеріалу лекції №3.	3	[24] с. 308-336, 371-386 [50] [51] [52] [53]
6	-	**ЛР3.** Підгрупа 2.	Підготовка до захисту лабораторної роботи №2. Підготовка до виконання лабораторної роботи №3.	4	[29] с. 42-63 [31] с. 195-214

7	**Тема 1. Моделювання та оцінювання безпеки систем** Міжнародні стандарти і практики оцінювання безпеки систем	**ЛР4.** Оцінювання ефективності систем та засобів кіберзахисту	Опрацювання теоретичного матеріалу лекції №4.	3	[25] [26] с. 108-134 [46]
8	-	**ЛР4.** Підгрупа 2.	Підготовка до захисту лабораторної роботи №3. Підготовка до виконання лабораторної роботи №4.	4	[29] с. 42-63 [31] с. 195-214 [51] [52] [53]
9	**Тема 2. Менеджмент та аудит інформаційної безпеки** Аналіз загроз безпеки	**ЛР5.** Моделювання атак і контрзаходів	Опрацювання теоретичного матеріалу лекції №5.	3	[7] с. 6-35 [23] с. 65-82 [24] с. 304-308 [35] [36] [45]
10	-	**ЛР5.** Підгрупа 2.	Підготовка до захисту лабораторної роботи №4. Підготовка до виконання лабораторної роботи №5.	4	[47] [48] [49] [51] [52] [53]
11	**Тема2. Менеджмент та аудит інформаційної безпеки** Управління інформаційною безпекою	**ЛР6.** Аналіз захищеності інформації при несанкціонованому доступі	Опрацювання теоретичного матеріалу лекції №6.	3	[17] [18] [19] [20] с. 9-127
12	-	**ЛР6.** Підгрупа 2.	Підготовка до захисту лабораторної роботи №5. Підготовка до виконання лабораторної роботи №6.	4	[24] с. 304-308 [47] [48] [49]
13	**Тема 2. Менеджмент та аудит інформаційної безпеки** Ризик-менеджмент інформаційної безпеки	**ЛР7.** Розробка системи управління інформаційною безпекою підприємства	Опрацювання теоретичного матеріалу лекції №7.	3	[20] с.128-240 [21] [22] [44]
14	-	**ЛР7.** Підгрупа 2.	Підготовка до захисту лабораторної роботи №6. Підготовка до виконання лабораторної роботи №7.	5	[20] с. 83-127 [24] с. 304-308
15	**Тема 2. Менеджмент та аудит інформаційної безпеки** Внутрішній аудит СМІБ	**ЛР8.** Управління ризиками інформаційної безпеки з використанням програмних засобів	Опрацювання теоретичного матеріалу лекції №8.	3	[12] с. 7-95 [20] с. 383-407

16	-	**ЛР8.** Підгрупа 2.	Підготовка до захисту лабораторної роботи №7. Підготовка до виконання лабораторної роботи №8.	5	[20] с. 83-127, 212-233
17	**Тема 2. Менеджмент та аудит інформаційної безпеки** Комплексний аудит інформаційної безпеки	-	Опрацювання теоретичного матеріалу лекції №9.	3	[16] с. 95-116 [20] с. 383-407
18	-	Підсумкове заняття **Контрольна робота**	Підготовка до контрольної роботи за пройденим матеріалом. Підготовка до захисту лабораторної роботи №8.	5	[20] с. 212-233

*** лекції проводяться по 2 години раз на два тижні;**
**** лабораторні проводяться по 4 години раз в два тижні.**

ПОЛІТИКА ДИСЦИПЛІНИ

Організація освітнього процесу з дисципліни відповідає вимогам положень про організаційне і навчально-методичне забезпечення освітнього процесу, освітній програмі та навчальному плану. Студент зобов'язаний відвідувати лекції і лабораторні заняття згідно з розкладом, не запізнюватися на заняття, вчасно виконувати та здавати лабораторні роботи. Термін виконання лабораторної роботи вважається своєчасним, якщо студент здав/захистив її на поточному або наступному за ним занятті. За несвоєчасний захист лабораторної роботи з набраної студентом суми балів вираховується один бал. Пропущене з поважної причини лабораторне заняття студент повинен відпрацювати у встановлений викладачем термін.

Виконуючи усі навчальні завдання з дисципліни, студент має дотримуватися політики доброчесності. У разі наявності плагіату він отримує незадовільну оцінку і має виконати завдання за новою темою.

Набуті особою знання з дисципліни або її окремих розділів у неформальній освіті зараховуються відповідно до Положення про порядок визнання та перезарахування результатів навчання здобувачів вищої освіти у ХНУ.

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 за ваговими коефіцієнтами (І семестр)

	Аудиторна робота	**Контрольні заходи**	**Підсумковий контрольний захід**
Вид заняття	Лабораторні роботи	Контрольна робота	Семестровий контроль (іспит)
Тема	1-2	1-2	1-2
Ваговий коефіцієнт	0,35	0,25	0,4

Структурування дисципліни за видами робіт і оцінювання результатів навчання студентів за ваговими коефіцієнтами (ІІ семестр)

	Аудиторна робота	**Контрольні заходи**	**Підсумковий контрольний захід**
Вид заняття	Лабораторні роботи	Контрольна робота	Семестровий контроль (іспит)
Тема	1-2	1-2	1-2
Ваговий коефіцієнт	0,35	0,25	0,4

Оцінювання лабораторних робіт. Оцінка, яка виставляється за лабораторну роботу, складається з таких елементів: знання теоретичного матеріалу з теми; якість оформлення звіту; вільне володіння студентом спеціальною термінологією і уміння професійно обґрунтувати прийняті конструктивні 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 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 лабораторну роботу викладач оголошує одразу після захисту звіту і проставляє в електронний журнал дисципліни.

Оцінювання контрольних робіт. Контрольна робота складається з двох теоретичних питань. Оцінювання здійснюється за чотирибальною шкалою.

Оцінку «відмінно» отримує студент який дав повну письмову відповідь на теоретичні питання.

Оцінку «добре» отримує студент, який дав правильну відповідь на теоретичні питання, але у відповіді присутні дві-три несуттєві помилки.

Оцінку «задовільно» отримує студент, який дав часткову відповідь на теоретичні питання.

Оцінку «незадовільно» отримує студент, який не дав відповіді на теоретичні питання.

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

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 матеріалу з дисципліни оцінюється за наведеними в таблиці критеріями.

Критерії оцінювання знань студентів

Оцінка за інституційною шкалою	**Узагальнений критерій**
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. Аналіз мережного трафіку.
2. Аналіз захищеності на рівні вузла
3. Спеціалізовані засоби аналізу захищеності.
4. Джерела даних для систем виявлення атак.
5. Ознаки атак
6. Методи виявлення атак
7. Принципи збору інформації для системи виявлення і блокування атак
8. Інтеграція засобів виявлення і запобігання атак в єдину систему і взаємодія з іншими засобами захисту
9. Основи планування безперервності роботи інформаційних систем
10. Поняття та класифікація інцидентів інформаційної безпеки відповідно до міжнародних стандартів та рекомендацій
11. Модель PDCA опису життєвого циклу процесів управління інцидентами інформаційної безпеки.
12. Особливості організації та функціонування команд (груп) CERT/CSIRT
13. Інструментарій для ефективного функціонування груп реагування на інциденти ІБ.
14. Документаційне забезпечення процесу управління інцидентами ІБ.
15. Діяльність різних груп реагування на інциденти ІБ.
16. Механізми реагування на інциденти
17. Методи соціального інжинірингу.
18. Основні алгоритми соціотехнічних атак на інформаційні ресурси
19. Етапи їх проведення соціотехнічних атак на інформаційні ресурси.
20. Рекомендації щодо захисту від соціотехнічних атак.
21. Менеджмент персоналу у сфері інформаційної безпеки.
22. Система менеджменту інформаційної безпеки
23. Загальні правила, положення та функції технологічного управління безпекою підприємства
24. Основні методи оцінки та аналізу інформаційних ризиків.
25. Стандарт NIST 800-30 та ISO 27002.
26. Класифікація ризиків інформаційної безпеки.
27. Методика, технології, Інструментальні засоби аналізу ризиків
28. Загальні принципи аудиту інформаційної безпеки.
29. Цілі та методи проведення зовнішнього аудиту
30. Аудит систем менеджменту інформаційної безпеки
31. Удосконалення системи інформаційної безпеки підприємства за допомогою страхування
32. Налаштування мережного середовища для моніторингу
33. Вибір мережевого відгалужувача
34. Моніторинг зараження ARP-кешу
35. Дослідження подій та інцидентів, ведення журналів реєстрації
36. Модель системи управління інформаційною безпекою підприємства
37. Задачі захисту інформації, що розв’язуються за допомогою моделювання.
38. Основні теорії і методи моделювання систем та засобів захисту інформації.
39. Характеристичні особливості задач моделювання систем і засобі кіберзахисту.
40. Моделі аналізу систем захисту інформації
41. Моделі синтезу систем захисту інформації
42. Моделі управління систем захисту інформації
43. Математичні моделі інформаційної безпеки
44. Системний підхід в моделях захисту інформації, ідентифікація системи і процесу
45. Оцінювання повноти та достовірності вихідних даних при моделюванні систем і засобів кіберзахисту

46. Дерева атак і контрзаходів
47. Графи шляхів реалізації атаки
48. Графи загроз
49. Граф-моделі об’єктів захисту
50. Постановка задачі оцінювання ефективності системи кіберзахисту.
51. Вибір критеріїв оцінювання ефективності системи кіберзахисту.
52. Аналітичний метод оцінювання систем захисту інформації
53. Теоретичний метод оцінювання систем захисту інформації
54. Аналітико-емпіричний метод оцінювання систем захисту інформації
55. Оцінювання систем і засобів кіберзахисту методами теорії ігор
56. Оцінювання захищеності інформації на основі «Матриці» Домарєва
57. Оцінювання захищеності інформації відповідно до ISO 13335
58. Методика оцінювання систем захисту інформації від Microsoft
59. Оцінювання загроз за методом STRIDE
60. Модель оцінювання DREAD

МЕТОДИЧНЕ ЗАБЕЗПЕЧЕННЯ

Навчальний процес з дисципліни повністю і в достатній кількості забезпечений необхідною навчально-методичною літературою, яка розміщена в модульному середовищі MOODLE.

РЕКОМЕНДОВАНА ЛІТЕРАТУРА

Основна

1. Опорний конспект лекцій з дисципліни «Моніторинг мережевої безпеки» для студентів напряму підготовки кібербезпека освітнього рівня магістр/Тернопільський національний економічний університет. Уклад. В.В. Яцків, І.З.Якименко. Тернопіль, ФОП Шпак В., 2019. 68 с.
2. Інформаційна безпека в комп'ютерних мережах: навч. посіб./ О.А. Смірнов, Конопліцька-О.К. Слободенюк, С.А. Смірнов, К.О. Буравченко, Т.В. Смірнова, Л.І. Поліщук. Кропивницький: Видавець Лисенко В. Ф., 2020. 295 с.
3. Апаратно-програмні засоби захисту інформації у корпораціях: навчально-методичний посібник. Вінниця: ДонНУ імені Василя Стуса, 2019. 36 с.
4. Технології моніторингу та трафік-інжинірингу в телекомунікаційних мережах: підручник П. В. Кучернюк; КПІ ім. Ігоря Сікорського. Київ : КПІ ім. Ігоря Сікорського, 2021. 257 с.
5. Технології захисту інформації в інформаційно-телекомунікаційних системах: навч. посіб./ А. В. Жилін, О. М. Шаповал, О. А. Успенський. ІСЗЗІ КПІ ім. Ігоря Сікорського. Київ: КПІ ім. Ігоря Сікорського, Вид-во «Політехніка», 2021. 213 с.
6. Управління інформаційною безпекою: навч. посіб./ С. О. Носок, О. М. Фаль, В. М. Ткач. Київ : КПІ ім. Ігоря Сікорського, 2021. 258 с.
7. Основи управління інформаційною безпекою: навч. посібник/ А.М. Гребенюк, Л.В. Рибальченко. Дніпро: Дніпроп. держ. унт внутріш. справ, 2020. 144 с.
8. Інформаційні технології. Методи захисту. Звід правил для управління інформаційною безпекою (ISO/IEC 27002:2010). 163 с.
9. Як налаштувати роботу CSIRT (команда реагування на інциденти комп'ютерної безпеки) та SOC (центр операційної безпеки) – керівництво з належної практики. Європейське Агентство з питань мережевої та інформаційної безпеки (ENISA), 2020. 57 с.
10. 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.
11. Information technology — Security techniques — Information security incident management (ISO/IEC 27035:2016, P.1, P. 2). 92 p.
12. Аудит та управління інцидентами інформаційної безпеки: навчальний посібник/ О.Г. Корченко, С.О. Гнатюк С.О, С.В. Казмірчук та ін. К.: Центр навч.-наук. та наук.-пр. видань НА СБ України, 2014. 190 с.
13. Основи кібербезпеки та кібероборони: підручник/ Ю.Г. Даник, П.П. Воробієнко, В.М. Чернега. Одеса.: ОНАЗ ім. О.С. Попова, 2019. 320 с.
14. Основи інформаційної безпеки: навч. пос./ Дудикевич В. Б., Хорошко В. О., Яремчук Ю. Є. Вінниця: ВНТУ, 2018. 316 с.
15. Що таке платформа MISP і як нею користуватися? [Електронний ресурс]. Режим доступу: https://kr-labs.com.ua/blog/shcho-take-platforma-misp
16. Learning Malware Analysis. Explore the concepts, tools, and techniques to analyze and investigate Windows malware Security/ Edited by Monnappa K A. Packt Publishing Ltd, 2018. 500 p.
17. ДСТУ ISO/IEC 27001:2023 (ISO/IEC 27001:2022, IDT). Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою.
18. ДСТУ ISO/IEC 27000:2019 (ISO/IEC 27000:2018, IDT). Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Огляд та словник термінів.
19. ДСТУ ISO/IEC 27003:2018 (ISO/IEC 27003:2017, IDT). Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Керівництво.

20. Менеджмент інформаційної безпеки: навчальний посібник/ О.Г. Корченко, М.Є. Шелест, С.В. Казмірчук, Ю.М. Ткач, Є.В. Іванченко. Ніжин: ФОП Лук'яненко В.В. ТПК «Орхідея», 2019. 408 с.

21. Guide for Conducting Risk Assessments NIST Special Publication 800-30 [Електронний ресурс]. Режим доступу: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

22. ДСТУ ISO/IEC 27005:2023 (ISO/IEC 27005:2022, IDT). Інформаційна безпека, кібербезпека та захист конфіденційності. Посібник з управління ризиками інформаційної безпеки.

23. Політики безпеки. Навчальний посібник/ Козачок В.А., Гайдур Г.І., Гахов С.О., Хмелевський Р.М., Чумак Н.С. Київ: ДУТ ННІЗІ, 2020. 167 с.

24. Моделювання систем захисту інформації: монографія/ А.О. Антонюк. Ірпінь: Національний університет ДПС України, 2015. 273 с.

25. Міжнародні стандарти ISO13335 і ISO15408 [Електронний ресурс]. Режим доступу: http://um.co.ua/8/8-2/8-207475.html

26. ISC2 CISSP® Certified Information Systems Security Professional: Official Study Guide. Eighth Edition/ Mike Chapple, James Michael, Stewart Darril Gibson. SYBEX, 2018. 1606 p.

27. Вступ в теорію систем: навчальний посібник/ І. В. Григоренко, С. І. Кондрашов, С. М. Григоренко. Харків: Факт, 2021. 202 с.

28. Моделювання складних систем: посібник/ Я.І. Виклюк, Р.М. Камінський, В.В. Пасічник. Львів: Видавництво «Новий Світ – 2000», 2020. 404 с.

29. Моделі структурного синтезу для управління параметрами інфокомунікаційних мереж систем критичної інфраструктури: монографія./ Косенко В. В., Невлюдов І. Ш. Х.: Харківський національний університет радіоелектроніки, 2019. 163 с.

30. Графи. як інструмент моделювання складних об'єктів та систем: навч. посіб./ О.А. Жученко, Т.А. Дунаєва. Київ : КПІ ім. Ігоря Сікорського, 2020. 68 с.

31. Discrete Probability Models and Methods. Probability on Graphs and Trees, Markov Chains and Random Fields, Entropy and Coding. /Pierre Brémaud. Cham, Switzerland: Springer, 2017. 561 p.

Додаткова

32. Моніторинг стану інформаційної безпеки сегментів корпоративних мереж сучасного бізнесу/ Н. В. Гуленко, Т. М. Яворська.// Вісник студентського наукового товариства ДонНУ імені Василя Стуса. Том 1 № 13 (2021). С. 252-255.

33. Security of IT outsourcing. Made by Danish IT Society's Group of IT Security Managers. 42 p.

34. Managing Information Security Outsourcing in a Dynamic Cooperation Environment/ Yong Wu, Giri Kumar Tayi, Genzhong Feng, Richard Y. K. Fung. Journal of the Association for Information Systems (2021) 22(3), 827-850. doi: 10.17705/1jais.00681

35. Класифікація моделей загроз в комп'ютерних системах/ В. Ю. Тітова, Ю. П. Кльоц, С.О. Савчук// Вісник Хмельницького національного університету. Технічні науки. 2020. № 2. С. 201-203.

36. Fuzzy Inference Subsystem for Classifying Threats to Computer Information/ V. Titova, Y. Klots, N. Petliak, M. Kapustian. International Scientific-technical journal «Measuring and computing devices in technological processes» 2022, Issue 1, PP. 57-61.

37. Застосування нейронних мереж у виявленні вторгнень/ В. Ю. Тітова, О. С. Андрощук, В. С. Даценко// Тези доповідей XVI Міжнародної науково-практичної конференції "Військова освіта і наука: сьогодення та майбутнє", 27 листоп. 2020 р. Київ: ВІКНУ, 2020. Т. 1. С. 62–63.

38. Research of the Neural Network Module for Detecting Anomalies in Network Traffic/ Klots, Y., Titova, V., Petliak, N., Cheshun, V., Salem, A.-B.M. CEUR Workshop Proceedings, 2022, 3156, PP. 378–389.

39. Signature-based Approach to Detecting Malicious Outgoing Traffic/ Petliak, N., Klots, Y., Titova, V., Cheshun, V., Boyarchuk, A. // CEUR Workshop Proceedings, 2023, 3373, PP. 486-506

40. Real-Time Information Security Incident Management: A Case Study Using the IS-CHEC Technique/ Mark Evans, Ying He, Cunjin Luo, Iryna Yevseyeva, Helge Janicke, Efpraxia Zamani, Leandros A. Maglaras. IEEE Access, Volume 7, 2019. PP. 142147-142175. https://doi.org/10.1109/access.2019.2944615

41. Security Operations & Incident Management Knowledge Area/ Hervé Debar, Howard Chivers. CyBOK, 2019. 47 p.

42. Observing Cyber Security Incident Response: Qualitative Themes From Field Research/ Megan Nyre-Yu, Robert S. Gutzwiller, Barrett S. Caldwell. - Proceedings of the Human Factors and Ergonomics Society 2019 Annual Meeting. PP. 437-441. https://doi.org/10.1177/1071181319631016

43. Open intrusion detection systems analysis/ Tereykovsky I., Korchenko A., Parashchuk T., Pedchenko Y.// Ukrainian Scientific Journal of Information Security, 2018, vol. 24, issue 3, PP. 201-216.

44. Security risk assessment within hybrid data centers: A case study of delay sensitive applications/ Fortune Munodawafa, Ali Ismail Awad. Journal of Information Security and Applications, Volume 43, December 2018. PP. 61-72. https://doi.org/10.1016/j.jisa.2018.10.008

45. Policy Management Engine (PME): A policy-based schema to classify and manage sensitive data in cloud storages/ Faraz Fatemi Moghaddam, Philipp Wieder, RaminYahyapour. Journal of Information Security and Applications, Volume 36, October 2017. pp. 11-19. https://doi.org/10.1016/j.jisa.2017.07.003

46. Підходи до побудови моделі загроз для аналізу безпеки відкритого програмного кода./ А.О Гапон., В.М. Федорченко, А.О. Поляков.// Системи обробки інформації. 2020. Випуск 1 (160). С. 128-135.

47. An evaluation of potential attack surfaces based on attack tree modelling and risk matrix applied to self-sovereign identity/ Nitin Naik, Paul Grace, Paul Jenkins, Kshirasagar Naik, Jingping Song.// Computers & Security. 2022. Vol. 120. P. 1-17.

48. Attack protection trees/ Aliyu Tanko Ali, Damas Gruska// Ceur-ws.org. 2019. Vol-2571. P. 1-12.

49. Reversible attack trees./ Aliyu Tanko Ali, Damas Gruska// Conference: 2021 IEEE 12th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON). 2021. P. 2-7.

50. Оптимізація методу вибору стратегії інвестування засобів захисту інформації на основі комбінації теорії ігор та генетичного алгоритму/ L..Plyska, & V. Maliukov.// Електронне фахове наукове видання "Кібербезпека: освіта, наука, техніка" 2022. №4(16). С. 172-184.

51. Методика оцінювання захищеності інформаційних систем за допомогою СУІБ «Матриця»/ Д. Домарєв, В. Домарєв// Захист інформації. 2013. Том 15, №1.С. 80-86.

52. Методика оцінки порушень захищеності інформаційних ресурсів в інформаційно-телекомунікаційних системах/ В.В. Сальник, О.А. Гуж, В.С. Закусіло, С.В. Сальник, П.В. Бєляєв. Збірник наукових праць Харківського національного університету Повітряних Сил. 2021. № 4(70). С. 77-82.

53. Оцінювання ефективності рішень в системах захисту інформації / В. Ю. Тітова, О. С. Андрощук, В. С. Орленко, І. М. Шевчук, В. С. Даценко// Вісник Хмельницького національного університету. Технічні науки. 2020. № 5. С. 307–310.

54. Модель безпеки поширення забороненої інформації в інформаційно-телекомунікаційних мережах/ С. В. Лєнков, В. М. Джулій, О. В. Селюков, В. С. Орленко, А. В. Атаманюк// Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. Київ: ВІКНУ, 2020. Вип. 68. С. 53-64.

ІНФОРМАЦІЙНІ РЕСУРСИ

1. Модульне середовище для навчання. URL : https://msn.khmnu.edu.ua/
2. Електронна бібліотека університету. URL: http://lib.khmnu.edu.ua/asp/php_f/p1age_lib.php