ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

ЗАТВЕРДЖУЮ
Декан факультету IT
_____ Олег САВЕНКО
Підпис Ім'я, ПРІЗВИЩЕ
«__» 08 2023 р.

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Управління інформаційною безпекою

Галузь знань	12 – Інформаційні технології
Спеціальність	125 – Кібербезпека
Рівень вищої освіти	Перший бакалаврський
Освітньо-професійна програма	Кібербезпека
Обсяг дисципліни	5 кредитів ЄКТС
Шифр дисципліни	ОПП.15
Мова навчання	Українська
Статус дисципліни	Обов'язкова, дисципліна професійної підготовки
Факультет	Інформаційних технологій
Кафедра	Кібербезпеки

Форма навчання	Курс	Семестр	Обсяг дисципліни		Кількість годин						Курсовий проєкт	Курсова робота	Форма семестрового контролю	
					Аудиторні заняття					Самостійна робота, у т.ч. ІРС				
			Кредити ЄКТС	Години	Разом	Лекції	Лабораторні роботи	Практичні заняття	Семінарські заняття				Залік	Іспит
Очна (денна)	4	7	5	150	51	34		17		99				+

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

Робоча програма складена _____ канд. техн. наук, доц. Віра ТІТОВА
Підпис(и) автора(ів) Ступінь, вчене звання, Ім'я, ПРІЗВИЩЕ автора(ів)

Схвалена на засіданні кафедри Кібербезпеки

Протокол від 31.08.2023 № 1 Зав. кафедри _____ Юрій КЛЬОЦ
Підпис Ім'я, ПРІЗВИЩЕ

Робоча програма розглянута та схвалена вченою радою факультету інформаційних технологій

Голова вченої ради факультету _____ Олег САВЕНКО
Підпис Ім'я, ПРІЗВИЩЕ

Хмельницький 2023

УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

Тип дисципліни	Обов'язкова
Освітній рівень	Перший (бакалаврський)
Мова викладання	Українська
Семестр	Сьомий
Кількість встановлених кредитів ЄКТС	5
Форми навчання, для яких викладається дисципліна	Очна денна

Студент, який успішно завершив вивчення дисципліни, повинен: *виявляти*, *ставити* та *вирішувати* проблеми у галузі управління інформаційною безпекою; *організовувати* власну професійну діяльність, *створювати* плани неперервності бізнесу згідно встановленої політики інформаційної та/або кібербезпеки для забезпечення безперервності бізнес-процесів організації на основі теорії ризиків та встановленої системи управління інформаційною безпекою, згідно з вітчизняними та міжнародними вимогами та стандартами; самостійно *застосовувати* законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі управління інформаційною безпекою, в тому числі, з метою розслідування внутрішніх та зовнішніх інцидентів інформаційної безпеки, *діяти* на основі законодавчої та нормативно-правової бази України і вимог відповідних стандартів (вітчизняних та міжнародних); *обирати* оптимальні методи та способи, аргументовано *приймати* рішення при розв'язанні складних спеціалізованих задач та практичних проблем у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, *оцінювати* ефективність прийнятих рішень; *управляти* інцидентами інформаційної та/або кібербезпеки, а саме: *виявляти*, *ідентифікувати*, *аналізувати* та *реагувати* на інциденти інформаційної та/або кібербезпеки, *впроваджувати* процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки; *автоматизовувати* зазначені процедури для забезпечення неперервності процесу ведення журналів реєстрації подій та інцидентів; *використовувати* сучасні методи і моделі інформаційної безпеки та/або кібербезпеки для вирішення задач управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах; *розробляти* та *впроваджувати* стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації, моделі і політику безпеки на основі використання сучасних принципів, способів та методів теорії захищених систем, *оцінювати* розроблені стратегії, моделі та політики; *застосовувати* різні класи політик інформаційної безпеки та/або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів; *здійснювати* професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою, в тому числі *готувати* пропозиції до нормативних актів щодо забезпечення інформаційної та/або кібербезпеки, *проводити* атестацію (спираючись на облік та обстеження) режимних територій (зон), приміщень тощо в умовах додержання режиму секретності із фіксуванням результатів у відповідних документах, тощо; *відновлювати* штатне, функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження з використанням процедур резервування згідно встановленої політики безпеки; *застосовувати* знання у практичних ситуаціях, *знати* та *використовувати* сучасні інформаційно-комунікаційні технології для адаптації в умовах частої зміни технологій управління інформаційною безпекою та прогнозування кінцевого результату управління; *використовувати* інструментарій для моніторингу процесів в інформаційно-телекомунікаційних системах

Зміст навчальної дисципліни: Основи управління ІБ. Правила управління ІБ: організація ІБ; управління активами; управління доступом; фізична та екологічна безпека; безпека операцій та зв'язку. Управління інцидентами ІБ. Аспекти ІБ при управлінні безперервністю бізнесу. Основи та поняття систем управління інформаційною безпекою (СУІБ). Вимоги до СУІБ. Розробка СУІБ. Аудит інформаційної безпеки підприємства. Ризик-менеджмент. Методика аналізу захищеності. Організація секретного діловодства. Адміністративний та процедурний рівні управління ІБ. Основи роботи з персоналом. Інформаційна безпека України. Організаційно-правові аспекти національної безпеки (НБ) України. Організаційно-правові аспекти забезпечення безпеки і стійкості критичної інфраструктури України.

Пререквізити: нормативно-правове забезпечення кібербезпеки.

Кореквізити: комплексні системи захисту інформації**,** переддипломна практика.

Запланована навчальна діяльність: лекцій 34, практичних занять 17 год., самостійної роботи 99 год., разом 150 год.

Методи навчання: словесні та наочні (лекції); практичні та частково-пошукові (практичні роботи); пояснювально-ілюстративні та дослідницькі (самостійна робота).

Форми оцінювання результатів навчання: вирішення практичних завдань, письмова контрольна робота, підсумковий контрольний захід.

Вид семестрового контролю: іспит.

Навчальні ресурси:
1. Основи інформаційної безпеки. Конспект лекцій/ Б.А. Заплотинський. КІВіП НУ "ОЮА, 2017. 128 с.
2. Інформаційна безпека держави: навчальний посібник./ В.І. Гур'єв, Д.Б. Мехед, Ю.М. Ткач, І.В. Фірсова. Ніжин: ФОП Лук'яненко В.В. ТПК «Орхідея», 2018. 166 с.
3. Інформаційна безпека: навчальний посібник / [Ю. Я. Бобало, І. В. Горбатий, М. Д. Кіселичник, А. П. Бондарєв та ін.]; за заг. ред. д-ра техн. наук, проф. Ю. Я. Бобала та д-ра техн. наук, доц. І. В. Горбатого. Львів: Видавництво Львівської політехніки, 2019. 580 с.
4. Модульне середовище для навчання MOODLE. Доступ до ресурсу: https://msn.khmnu.edu.ua
5. Електронна бібліотека університету. Доступ до ресурсу: http://lib.khmnu.edu.ua/asp/php_f/p1age_lib.php

Викладач: к.т.н., доц. Тітова В.Ю.

ВСТУП

Дисципліна «Управління інформаційною безпекою» - складова професійної підготовки бакалаврів зі спеціальності «Кібербезпека», є однією з профілюючих дисциплін.

Метою викладання навчальної дисципліни «Управління інформаційною безпекою» є формування у майбутніх спеціалістів умінь та компетенцій для забезпечення менеджменту інформаційної безпеки у комп'ютерних та інформаційно-комунікаційних системах; розвиток у студентів фахового стилю мислення; надання глибоких та міцних знань з питань управління інформаційною та кібербезпекою в умовах широкого використання сучасних інформаційних технологій.

Предметом дисципліни є організація систем управління інформаційною безпекою на основі міжнародних стандартів і практик; теорії, моделі та принципи управління доступом до інформаційних ресурсів; методи та засоби виявлення, управління та ідентифікації загроз та вразливостей; методи та засоби оцінювання та забезпечення необхідного рівня захищеності інформації.

Завданням дисципліни є забезпечити набуття компетентностей та досягнення програмних результатів навчання відповідно до Стандарту вищої освіти та освітньо-професійної програми підготовки бакалаврів зі спеціальності «Кібербезпека»:

***компетентності*:**

КЗ 1. Здатність застосовувати знання у практичних ситуаціях.

КЗ 4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням.

КФ 1. Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі інформаційної та/або кібербезпеки.

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

КФ 4. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки.

КФ 6. Здатність відновлювати штатне, функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження.

КФ 8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку

КФ 9. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою.

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

результати навчання:

РН 2. Організовувати власну професійну діяльність, обирати оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність.

РН 4. Аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач та практичних проблем у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення.

РН 5. Адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат.

РН 7. Діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та/або кібербезпеки.

РН 8. Готувати пропозиції до нормативних актів щодо забезпечення інформаційної та/або кібербезпеки.
РН 9. Впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки.
РН 24. Вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових).
РН 32. Вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки.
РН 34. Приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації.
РН 39. Проводити атестацію (спираючись на облік та обстеження) режимних територій (зон), приміщень тощо в умовах додержання режиму секретності із фіксуванням результатів у відповідних документах.
РН 41. Забезпечувати неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур.
РН 42. Впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки.
РН 43. Застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/ або кібербезпеки для розслідування інцидентів.
РН 44. Вирішувати задачі забезпечення безперервності бізнес-процесів організації на основі теорії ризиків та встановленої системи управління інформаційною безпекою, згідно з вітчизняними та міжнародними вимогами та стандартами.
РН 45. Застосовувати різні класи політик інформаційної безпеки та/або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів.
РН 52. Використовувати інструментарій для моніторингу процесів в інформаційно-телекомунікаційних системах.

Студент, який успішно завершив вивчення дисципліни, повинен: *виявляти, ставити* та *вирішувати* проблеми у галузі управління інформаційною безпекою; *організовувати* власну професійну діяльність, *створювати* плани неперервності бізнесу згідно встановленої політики інформаційної та/або кібербезпеки для забезпечення безперервності бізнес-процесів організації на основі теорії ризиків та встановленої системи управління інформаційною безпекою, згідно з вітчизняними та міжнародними вимогами та стандартами; самостійно *застосовувати* законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі управління інформаційною безпекою, в тому числі, з метою розслідування внутрішніх та зовнішніх інцидентів інформаційної безпеки, *діяти* на основі законодавчої та нормативно-правової бази України і вимог відповідних стандартів (вітчизняних та міжнародних); *обирати* оптимальні методи та способи, аргументовано *приймати* рішення при розв'язанні складних спеціалізованих задач та практичних проблем у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, *оцінювати* ефективність прийнятих рішень; *управляти* інцидентами інформаційної та/або кібербезпеки, а саме: *виявляти, ідентифікувати, аналізувати* та *реагувати* на інциденти інформаційної та/або кібербезпеки, *впроваджувати* процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки; *автоматизовувати* зазначені процедури для забезпечення неперервності процесу ведення журналів реєстрації подій та інцидентів; *використовувати* сучасні методи і моделі інформаційної безпеки та/або кібербезпеки для вирішення задач управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах; *розробляти* та *впроваджувати* стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації, моделі і політику безпеки на

основі використання сучасних принципів, способів та методів теорії захищених систем, *оцінювати* розроблені стратегії, моделі та політики; *застосовувати* різні класи політик інформаційної безпеки та/або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів; *здійснювати* професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою, в тому числі *готувати* пропозиції до нормативних актів щодо забезпечення інформаційної та/або кібербезпеки, *проводити* атестацію (спираючись на облік та обстеження) режимних територій (зон), приміщень тощо в умовах додержання режиму секретності із фіксуванням результатів у відповідних документах, тощо; *відновлювати* штатне, функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження з використанням процедур резервування згідно встановленої політики безпеки; *застосовувати* знання у практичних ситуаціях, *знати* та *використовувати* сучасні інформаційно-комунікаційні технології для адаптації в умовах частої зміни технологій управління інформаційною безпекою та прогнозування кінцевого результату управління; *використовувати* інструментарій для моніторингу процесів в інформаційно-телекомунікаційних системах.

СТРУКТУРА ЗАЛІКОВИХ КРЕДИТІВ ДИСЦИПЛІНИ

Назва теми	Кількість годин відведених на:		
	лекції	практичні заняття	самостійну роботу
Тема 1. Основи управління ІБ	6	-	6
Тема 2. Політики інформаційної безпеки	2	2	10
Тема 3. Системи управління інформаційною безпекою (СУІБ)	6	8	38
Тема 4. Моніторинг безпеки та реагування на кіберінциденти	16	4	32
Тема 5. Відновлення функціонування ІКС	4	3 (4/2)*	13 (12/14)*
Разом:	**34**	**17 (18/16)***	**99 (98/100)***

* За чисельником / за знаменником (розрахунок здійснюється відповідно до розкладу занять)

ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ
Зміст лекційного курсу

Номер лекції	Перелік тем лекцій, їх анотація	Години
Тема 1. Основи управління ІБ		
1	**Основи управління ІБ** 1. Поняття та термінологія управління ІБ 2. Об'єкти та складові управління ІБ 3. Важність і складність проблем управління ІБ Літ.: [1] с. 8-30; [3] с. 19-38; [4] с. 1-74	2
2	**Правила управління ІБ (частина 1)** 1. Організація ІБ 2. Безпека, пов'язана з персоналом 3. Управління активами 4. Управління доступом 5. Криптографія в задачах управління ІБ Літ.: [6] с. 1-37, с. 60-77; [12] с. 240-324	2
3	**Правила управління ІБ (частина 2)** 1. Фізична та екологічна безпека 2. Безпека операцій 3. Безпека зв'язку 4. Придбання, розробка, впровадження та супровід інформаційних систем 5. Взаємовідносини з постачальниками Літ.: [6] с. 37-60, с. 77-90; [12] с. 324-364	2
Тема 2. Політики інформаційної безпеки		
4	**Політики безпеки** 1. Поняття політики безпеки (ПБ). 2. Дискреційна ПБ. Мандатна ПБ. Рольова ПБ 3. Монітор безпеки. 4. Визначення та відомості, що мають міститися в ПБ. Дотримання ПБ. Літ.: [2] с. 114-123; [10] с. 55-95	2
Тема 3. Системи управління інформаційною безпекою (СУІБ)		
5	**Основи та поняття СУІБ** 1. Сфера застосування СУІБ 2. Терміни та визначення СУІБ 3. Сертифікація СУІБ Літ.: [7] с. 1-26; [12] с. 71-83	2
6	**Вимоги до СУІБ** 1. Планування СУІБ 2. Експлуатація СУІБ 3. Оцінка результативності СУІБ 4. Вдосконалення СУІБ Літ.: [5] с. 1-23; [12] с. 83-127	2
7	**Розробка СУІБ** 1. Визначення області дії, меж і політики СУІБ 2. Проведення аналізу вимог до ІБ 3. Проведення оцінювання і планування обробки ризиків 4. Основні процеси розробки СУІБ Літ.: [8] с. 1-45	2
Тема 4. Моніторинг безпеки та реагування на кіберінциденти		
8	**Моніторинг ІБ та SIEM** 1. Джерела інформації про події та типи подій	2

	2. Види та застосування систем SIEM. 3. Принцип роботи системи SIEM. 4. Приклади комерційних систем SIEM Літ.: [13] с. 4-24; [14] с. 1-65	
9	**Розуміння інцидентів кібербезпеки** 1. Основи реагування на кіберінциденти. 2. Визначення інциденту кібербезпеки. 3. Порівняння різних типів інцидентів кібербезпеки 4. Реагування на інциденти ІБ 5. Цілі процесу реагування Літ.: [13] с. 4-24; [14] с. 1-65	2
10	**Організація реагування та розслідування кіберінцидентів** 1. Створення політики, плану та процедур реагування на інциденти. 2. Елементи політики. Елементи плану. Елементи процедури. 3. Обмін інформацією із зовнішніми сторонами Літ.: [13] с. 4-24; [14] с. 1-65	2
11	**Структура групи реагування на інциденти** 1. Моделі команд. Вибір моделі команди. 2. Персонал реагування на інциденти. Залежності всередині організацій. 3. Служби групи реагування на інциденти Літ.: [13] с. 4-24; [14] с. 1-65	2
12	**Життєвий цикл атаки (Kill Chain)** 1. Розвідка та збір даних (Reconnaissance). 2. Вибір способу атаки (Weaponization). 3. Доставка (Delivery). Експлуатація (Exploitation). Закріплення (Installation). Виконання команд (Command and Control). 4. Досягнення мети (Actions on Objective) Літ.: [13] с. 4-24; [14] с. 1-65	2
13	**Опрацьовування інциденту (частина 1)** 1. Підготовка до врегулювання інцидентів. 2. Запобігання інцидентам. Виявлення та аналіз. 3. Вектори атаки. Ознаки події. Джерела прекурсорів та індикатори. 4. Аналіз інцидентів. Документація про інцидент. Пріоритизація інцидентів. 5. Повідомлення про інцидент. Стримування, викорінення та відновлення. Вибір стратегії стримування. Літ.: [13] с. 4-24; [14] с. 1-65	2
14	**Опрацьовування інциденту (частина 2)** 1. Збір та обробка доказів. Ідентифікація атакуючих хостів. 2. Викорінення та відновлення. Події після інциденту. 3. Використання зібраних даних про інциденти. 4. Зберігання доказів. 5. Контрольний перелік обробки інцидентів. Літ.: [13] с. 4-24; [14] с. 1-65	2
15	**Координація та обмін інформацією** 1. Координаційні відносини. Угоди про спільне використання та вимоги до звітності. 2. Методи обміну інформацією (спеціальні, частково автоматизовані). 3. Питання безпеки. Обмін детальною інформацією. 4. Інформація про вплив на бізнес. Технічна інформація. Рекомендації. Літ.: [13] с. 4-24; [14] с. 1-65	2
Тема 5. Відновлення функціонування ІКС		
16	**Організаційно-технічні заходи відновлення функціонування ІКС** 1. Аварія як можливий стан ІКС 2. Завдання аварійного планування та стадії відновлювальних робіт після	2

	аварії ІКС 3. Журнал аудиту подій Літ.: [1] с. 119-127; [9] с. 7-33; [12] с. 383-407	
17	**Резервування ресурсів ІКС та резервне зберігання даних** 1. Вимоги до систем резервного копіювання 2. Види резервного копіювання 3. Схеми ротації 4. Методи боротьби з втратою даних 5. Політики резервного копіювання даних Літ.: [2] с. 74-92; [11] с. 24-38	2
	Разом за семестр:	**34**

Зміст практичних занять

№ п/п	**Теми занять**	**Кількість годин**
1	Ідентифікація та оцінювання інформаційних активів підприємства	2
2	Ідентифікація загроз, вразливостей та їх джерел	2
3	Створення моделі управління інформаційною безпекою підприємства за допомогою програмного комплексу Coras	2
4	Розробка політики безпеки для корпоративної мережі підприємства	2
5	Оцінювання політики безпеки інформаційної системи підприємства на відповідність стандартам безпеки	2
6	Встановлення та налаштування IBM QRadar SIEM	2
7	Дослідження подій та інцидентів на підприємстві за допомогою IBM QRadar SIEM, ведення журналів реєстрації	2
8	Ізоляція інфікованих машин. Викорінення та відновлення. Складання звіту.	2
9	Підсумкове заняття. Контрольна робота	1 (2/1)*
	Разом за семестр:	**17 (18/16)***

* За чисельником / за знаменником (розрахунок здійснюється відповідно до розкладу занять)

Зміст самостійної (у т.ч. індивідуальної) роботи

Об’єм самостійної роботи з дисципліни “Управління інформаційною безпекою” становить 99 годин. Він включає опрацювання лекційного матеріалу та літературних джерел, підготовку до контрольної роботи, виконання практичних завдань та створення презентацій для демонстрації результатів виконання. Керівництво самостійною роботою здійснює викладач згідно з розкладом консультацій в позаурочний час.

Номер тижня	Вид самостійної роботи	Кількість годин
1	Опрацювання теоретичного матеріалу лекції №1. Виконання завдань практичного заняття №1.	5
2	Опрацювання теоретичного матеріалу лекції №2.	5
3	Опрацювання теоретичного матеріалу лекції №3. Виконання завдань практичного заняття №2.	6
4	Опрацювання теоретичного матеріалу лекції №4.	6
5	Опрацювання теоретичного матеріалу лекції №5. Виконання завдань практичного заняття №3.	6
6	Опрацювання теоретичного матеріалу лекції №6.	6
7	Опрацювання теоретичного матеріалу лекції №7. Виконання завдань практичного заняття №4.	6
8	Опрацювання теоретичного матеріалу лекції №8.	6
9	Опрацювання теоретичного матеріалу лекції №9. Виконання завдань практичного заняття №5.	6
10	Опрацювання теоретичного матеріалу лекції №10.	6
11	Опрацювання теоретичного матеріалу лекції №11. Виконання завдань практичного заняття №6.	6
12	Опрацювання теоретичного матеріалу лекції №12.	7 (6/7)*
13	Опрацювання теоретичного матеріалу лекції №13. Виконання завдань практичного заняття №7.	6
14	Опрацювання теоретичного матеріалу лекції №14.	6 (6/7)*
15	Опрацювання теоретичного матеріалу лекції №15. Виконання завдань практичного заняття №8.	6
16	Опрацювання теоретичного матеріалу лекції №16.	6
17	Опрацювання лекційного матеріалу по лекції №17. Підготовка до контрольної роботи за пройденим матеріалом.	4
	Разом за семестр:	99 (98/100)*

* При плануванні практичних занять за чисельником/ за знаменником (розрахунок здійснюється відповідно до розкладу занять)

ТЕХНОЛОГІЇ ТА МЕТОДИ НАВЧАННЯ

Процес навчання з дисципліни ґрунтується на використанні традиційних та сучасних методів. Зокрема, лекції проводяться пояснювально-ілюстративними, тренінговими та проблемними методами з супроводом презентаційних матеріалів, практичні заняття проводяться практичними, продуктивними, проблемними, контекстними методами з використанням сучасних інформаційно-комп'ютерних технологій (MS Security Assessment Tool, IBM Qradar та інших) і мають за мету – набуття студентами практичних навичок управління інформаційною та кібербезпекою.

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

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

МЕТОДИ КОНТРОЛЮ

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

При цьому використовуються такі методи поточного контролю:

- вирішення практичних завдань;
- письмова контрольна робота.

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

ОЦІНЮВАННЯ РЕЗУЛЬТАТІВ НАВЧАННЯ СТУДЕНТІВ

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

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

	Аудиторна робота	**Контрольні заходи**	**Підсумковий контрольний захід**
Вид заняття	Практичні заняття (мінімальна кількість оцінок - 8)	Контрольна робота	Семестровий контроль (іспит)
Тема	1-5	1-5	1-5
Ваговий коефіцієнт	0,4	0,2	0,4

Оцінювання практичних занять. Оцінка, яка виставляється за практичне заняття, складається з таких елементів: знання теоретичного матеріалу з теми; якість оформлення презентації виконаного завдання; вільне володіння студентом спеціальною термінологією і уміння застосовувати знання на практиці; своєчасна здача практики.

Термін здачі практики вважається своєчасним, якщо студент здав її в день виконання або на наступному після виконання завдання занятті. Пропущене заняття студент зобов'язаний відпрацювати в аудиторіях 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 практичне заняття викладач оголошує одразу після здачі і проставляє в електронний журнал дисципліни.

Оцінювання контрольних робіт. Контрольна робота складається з теоретичного питання та практичного завдання за темою одного з практичних занять. Оцінювання здійснюється за чотирибальною шкалою.

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

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

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

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

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

Семестровий контроль (іспит). Підсумковий контрольний захід з дисципліни проводиться в формі іспиту. Екзаменаційний білет складається з теоретичного питання 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. Поняття та термінологія управління ІБ.
2. Об’єкти та складові управління ІБ.
3. Важливість і складність проблем управління ІБ.
4. Правила управління ІБ: організація ІБ.
5. Правила управління ІБ: безпека, пов'язана з персоналом.
6. Правила управління ІБ: управління активами.
7. Правила управління ІБ: управління доступом.
8. Правила управління ІБ: криптографія.
9. Правила управління ІБ: безпека операцій.
10. Правила управління ІБ: безпека зв'язку.
11. Правила управління ІБ: купівля, розробка та супровід інформаційних систем (ІС).
12. Правила управління ІБ: взаємовідносини з постачальниками.
13. Управління інцидентами ІБ.
14. Виявлення інцидентів ІБ.
15. Реєстрація інцидентів ІБ.
16. Реагування на інциденти ІБ.
17. Розслідування інцидентів ІБ та збір правових доказів.
18. Аспекти ІБ при управлінні безперервністю бізнесу.
19. Основи та поняття СУІБ.
20. Сфера застосування СУІБ.
21. Терміни та визначення СУІБ.
22. Сертифікація СУІБ.
23. Вимоги до СУІБ.
24. Цілі і засоби СУІБ.
25. Визначення області дії, меж і політики СУІБ.
26. Проведення аналізу вимог до ІБ.
27. Основні процеси розробки СУІБ.
28. Проведення аналізу вимог до ІБ.
29. Надання послуг в сфері інформаційної безпеки.
30. Програмна підтримка роботи з політикою безпеки.
31. Програмні засоби, що інтегруються в СУІБ підприємства.
32. Аудит стану інформаційної безпеки на підприємстві.
33. Модель СУІБ підприємства.
34. Етапність аудиту інформаційної безпеки.
35. Оцінка відповідності ІС вимогам стандартів.
36. Методика аналізу захищеності інформаційних активів.
37. Передумови розвитку менеджменту в сфері інформаційної безпеки.
38. Загальна структура управлінської роботи по забезпеченню інформаційної безпеки на підприємстві.
39. Віднесення відомостей до комерційної таємниці.
40. Віднесення відомостей до державної таємниці.
41. Організація доступу до таємної інформації.
42. Захист службової інформації.
43. Адміністративний рівень управління ІБ.
44. Процедурний рівень управління ІБ.
45. Реагування на порушення режиму безпеки.
46. Планування відновлювальних робіт.
47. Права працівників на доступ до серверів і баз даних колективного використання.
48. Департамент інформаційної безпеки.
49. Планування персоналу.

50. Етапи формування трудового колективу.
51. Організація допуску персоналу до конфіденційної інформації.
52. Забезпечення ІБ України.
53. Система та політика забезпечення ІБ України.
54. ІБ України у сфері прав і свобод людини.
55. Основні напрями державної політики з питань НБ України.
56. Місце і роль ІБ в системі НБ держави.
57. Система безпеки та стійкості критичної інфраструктури.
58. Методологічні засади забезпечення безпеки та стійкості критичної інфраструктури.
59. Організаційні засади забезпечення безпеки та стійкості критичної інфраструктури.
60. Суб’єкти інформаційного простору України.

МЕТОДИЧНЕ ЗАБЕЗПЕЧЕННЯ

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

РЕКОМЕНДОВАНА ЛІТЕРАТУРА

Основна

1. Основи інформаційної безпеки. Конспект лекцій/ Б.А. Заплотинський. – КІІВіП НУ "ОЮА", 2017. – 128 с.
2. Інформаційна безпека держави: навчальний посібник/ В.І. Гур'єв, Д.Б. Мехед, Ю.М. Ткач, І.В. Фірсова. – Ніжин: ФОП Лук'яненко В.В. ТПК «Орхідея», 2018. – 166 с.
3. Інформаційна безпека: навчальний посібник/ Ю. Я. Бобало, І. В. Горбатий, М. Д. Кіселичник, А. П. Бондарєв, С. С. Войтусік, А. Я. Горпенюк, О. А. Нємкова, І. М. Журавель, Б. М. Березюк, Є. І. Яковенко, В. І. Отенко, І. Я. Тишик; за заг. ред. д-ра техн. наук, проф. Ю. Я. Бобала та д-ра техн. наук, доц. І. В. Горбатого. – Львів: Видавництво Львівської політехніки, 2019. – 580 с.
4. ISO/IEC 15408. Information technology – Security techniques – Evaluation criteria for IT security – Part 1: Introduction and general model. – ISO: Geneva, 2009. – 74 p.
5. ISO/IEC 27001:2013. Information technology – Security techniques – Information security management systems – Requirements. – ISO: Geneva, 2013. – 32 p.
6. ISO/IEC 27002:2013. Information technology – Security techniques – Code of practice for information security management. – ISO: Geneva, 2013. – 136 p.
7. ISO/IEC 27000:2018. Information technology – Security techniques – Information security management systems – Overview and vocabulary. – ISO: Geneva, 2018. – 34 p.
8. ISO/IEC 27003:2017. Information technology – Security techniques – Information security management systems – Guidance. – ISO: Geneva, 2017. – 76 p.
9. 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.
10. Інформаційна безпека: питання правового регулювання: монографія/ А.Ю. Нашинець-Наумова. – К.: Видавничий дім «Гельветика», 2017. – 168 с.
11. Інформаційна безпека держави: навчальний посібник/ Т.М.Мужанова. – К.: ДУТ, 2019. – 131 с.
12. 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.
13. Апаратно-програмні засоби захисту інформації у корпораціях: навчально-методичний посібник [Електронний ресурс]/ В.Г. Крижановський, С.П. Сергієнко. – Вінниця : ДонНУ імені Василя Стуса, 2019. – режим доступу: https://r.donnu.edu.ua/bitstream/123456789/111/1/Методичка%20Засоби%20захисту%20інформації%20у%20корпораціях.pdf
14. IBM QRadar. Installation Guide [Електронний ресурс]. – IBM Corp., 2019. – режим доступу: https://www.ibm.com/support/knowledgecenter/SS42VS_7.3.3/com.ibm.qradar.doc/b_siem_inst.pdf

Додаткова

17. Practical Information Security Management: A Complete Guide to Planning and Implementation/ Tony Campbell. – Australia: Burns Beach, 2016. – 253 p.
18. Розроблення політики інформаційної безпеки приватного підприємства/ Тітова Віра, Кльоц Юрій, Петляк Наталія, Огородник Максим// International Scientific-technical journal «Measuring and computing devices in technological processes» 2023, Issue 3 С.228-232
19. Safeguarding the Information Systems in an Organization through Different Technologies, Policies, and Actions/ Hend K. Alkahtani. – Computer and Information Science. – Vol. 12, No. 2; 2019. – Published by Canadian Center of Science and Education. – P. 117-125.

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