ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

ЗАТВЕРДЖУЮ

Декан факультету інформаційних технологій

_____ Тетяна ГОВОРУЩЕНКО
Підпис Ім'я, ПРІЗВИЩЕ

29 серпня 2025 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.17
Мова навчання – Українська
Статус дисципліни– Обов'язкова (фахової підготовки)
Факультет – Інформаційних технологій
Кафедра – Кібербезпеки

Форма здобуття освіти	Курс	Семестр	Загальний обсяг		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
Д	4	7	5	150	50	32	18	-	-	100	-	-	-	+
Разом ДФН			**5**	**150**	**50**	**32**	**18**	**-**	**-**	**100**	**-**	**-**	**-**	**1**

Робоча програма складена на основі освітньо-професійної програми «Кібербезпека» за спеціальністю 125 «Кібербезпека»

Робоча програма складена _____ канд. техн. наук, доцент Віра ТІТОВА
Підпис автора(ів) Науковий ступінь, вчене звання, Ім'я, ПРІЗВИЩЕ автора(ів)

Схвалена на засіданні кафедри Кібербезпеки

Протокол від 29.08.2025 № 1. Зав. кафедри _____ Юрій КЛЬОЦ
Підпис Ім'я, ПРІЗВИЩЕ

Робоча програма розглянута та схвалена вченою радою факультету інформаційних технологій

Голова вченої ради факультету _____ Тетяна ГОВОРУЩЕНКО
Підпис Ім'я, ПРІЗВИЩЕ

Хмельницький 2025

ЛИСТ ПОГОДЖЕННЯ

Посада	Назва кафедри	Підпис	Ініціали, прізвище
Завідувач кафедри, канд. техн. наук, доц.	Кібербезпеки		Юрій КЛЬОЦ
Гарант освітньо-професійної програми, канд. техн. наук, доц.	Кібербезпеки		Віктор ЧЕШУН

3. ПОЯСНЮВАЛЬНА ЗАПИСКА

Дисципліна «Управління інформаційною безпекою» є однією із дисциплін фахової підготовки здобувачів першого (бакалаврського) рівня вищої освіти, очної (денної) форми здобуття вищої освіти, які навчаються за освітньо-професійною програмою «Кібербезпека» в межах спеціальності 125 «Кібербезпека».

***Пререквізити*:** нормативно-правове забезпечення кібербезпеки.

***Постреквізити*:** комплексні системи захисту інформації; переддипломна практика.

Відповідно до освітньої програми дисципліна сприяє забезпеченню:

***компетентностей*:** ІК Здатність розв'язувати складні спеціалізовані задачі та практичні проблеми у галузі забезпечення інформаційної безпеки і/або кібербезпеки, що характеризуються комплексністю та неповною визначеністю умов; ЗК 1 Здатність застосовувати знання у практичних ситуаціях; ЗК 4 Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням; ФК 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; ФК 2 Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки; ФК 4 Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки; ФК 6 Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження; ФК 8 Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку; ФК 9 Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою; ФК 11 Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки.

***програмних результатів навчання*:** ПРН 2 Організовувати власну професійну діяльність, обирати оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність; ПРН 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; ПРН 5 Адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат; ПРН 7 Діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та/або кібербезпеки; ПРН 8 Готувати пропозиції до нормативних актів щодо забезпечення інформаційної та/або кібербезпеки; ПРН 9 Впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки; ПРН 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); ПРН 32 Вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки; ПРН 34 Приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації; ПРН 39 Проводити атестацію (спираючись на облік та обстеження) режимних територій (зон), приміщень тощо в умовах додержання режиму секретності із фіксуванням результатів у відповідних документах; ПРН 41 Забезпечувати неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур; ПРН 42 Впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки; ПРН 43 Застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/або кібербезпеки для розслідування інцидентів; ПРН 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; ПРН 45 Застосовувати різні класи політик інформаційної безпеки та/або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів; ПРН 52 Використовувати інструментарій для моніторингу процесів в інформаційно-телекомунікаційних системах.

Мета дисципліни. Формування у здобувачів системних знань і практичних навичок з управління інформаційною та кібербезпекою в умовах широкого використання сучасних інформаційних технологій.

Предмет дисципліни. 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.

Завдання дисципліни. Формування у майбутніх спеціалістів умінь, навичок та компетентностей для забезпечення менеджменту інформаційної безпеки у комп'ютерних та інформаційно-комунікаційних системах та реагування на кіберінциденти.

Результати навчання. Після вивчення дисципліни студент повинен: *виявляти*, *формулювати* та *вирішувати* проблеми в управлінні інформаційною безпекою, *організовувати* професійну діяльність, *планувати* неперервність бізнесу згідно з політикою безпеки та стандартами; самостійно *застосовувати* законодавчу й нормативну базу, *розслідувати* інциденти, *приймати* обґрунтовані рішення в складних умовах, *оцінювати* їхню ефективність; *здійснювати* управління інцидентами кібербезпеки, *автоматизувати* процеси моніторингу подій, *використовувати* сучасні моделі безпеки для керування доступом, *розробляти* стратегії кіберзахисту, *впроваджувати* політики, *готувати* нормативні пропозиції, *проводити* атестацію об'єктів; *відновлювати* роботу систем після інцидентів, *застосовувати* сучасні ІКТ і *прогнозувати* результати управління.

4. СТРУКТУРА ЗАЛІКОВИХ КРЕДИТІВ ДИСЦИПЛІНИ

Назва теми	Кількість годин відведених на:		
	лекції	**практичні заняття**	**СРС**
Тема 1. Основи управління ІБ	6	-	6
Тема 2. Політики інформаційної безпеки	2	4	12
Тема 3. Системи управління інформаційною безпекою (СУІБ)	4	6	18
Тема 4. Моніторинг безпеки та реагування на кіберінциденти	16	4	48
Тема 5. Відновлення функціонування ІКС	4	4	16
Разом:	**32**	**18**	**100**

5. ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

5.1 Зміст лекційного курсу

Номер лекції	Перелік тем лекцій, їх анотації	Кількість годин
	Тема 1. Основи управління ІБ	
1	**Основи управління ІБ** Поняття та термінологія управління ІБ. Об’єкти та складові управління ІБ. 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)** Організація ІБ. Безпека, пов'язана з персоналом. Управління активами. Управління доступом. Криптографія в задачах управління ІБ. Літ.: [6]; [12]	2
3	**Правила управління ІБ (частина 2)** Фізична та екологічна безпека. Безпека операцій. Безпека зв'язку. Придбання, розробка, впровадження та супровід інформаційних систем. Взаємовідносини з постачальниками. Літ.: [6]; [12]	2
	Тема 2. Політики інформаційної безпеки	
4	**Політики безпеки** Поняття політики безпеки (ПБ). Дискреційна ПБ. Мандатна ПБ. Рольова ПБ. Монітор безпеки. Визначення та відомості, що мають міститися в ПБ. Дотримання ПБ. Літ.: [2] с. 114-123; [10]	2
	Тема 3. Системи управління інформаційною безпекою (СУІБ)	
5	**Основи та поняття СУІБ. Вимоги до СУІБ** Сфера застосування СУІБ. Терміни та визначення СУІБ. Сертифікація СУІБ. Планування СУІБ. Експлуатація СУІБ. Оцінка результативності СУІБ. Вдосконалення СУІБ Літ.: [7]; [12]	2
6	**Розробка СУІБ** Визначення області дії, меж і політики СУІБ. Проведення аналізу вимог до ІБ. Проведення оцінювання і планування обробки ризиків. Основні процеси розробки СУІБ Літ.: [8]	2
	Тема 4. Моніторинг безпеки та реагування на кіберінциденти	
7	**Моніторинг ІБ та SIEM** Джерела інформації про події та типи подій. Види та застосування систем SIEM. Принцип роботи системи SIEM. Приклади комерційних систем SIEM. Літ.: [13]; [14]	2
8	**Розуміння інцидентів кібербезпеки** Основи реагування на кіберінциденти. Визначення інциденту кібербезпеки. Порівняння різних типів інцидентів кібербезпеки. Реагування на інциденти ІБ. Цілі процесу реагування. Літ.: [13]; [14]	2
9	**Організація реагування та розслідування кіберінцидентів** Створення політики, плану та процедур реагування на інциденти. Елементи політики. Елементи плану. Елементи процедури. Обмін інформацією із зовнішніми сторонами. Літ.: [13]; [14]	2
10	**Структура групи реагування на інциденти** Моделі команд. Вибір моделі команди. Персонал реагування на інциденти. Залежності всередині організацій. Служби групи реагування на інциденти. Літ.: [13]; [14]	2
11	**Життєвий цикл атаки (Kill Chain)** Розвідка та збір даних (Reconnaissance). Вибір способу атаки (Weaponization). Доставка (Delivery). Експлуатація (Exploitation). Закріплення (Installation). Виконання команд (Command and Control). Досягнення мети (Actions on Objective). Літ.: [13]; [14]	2
12	**Опрацьовування інциденту (частина 1)** Підготовка до врегулювання інцидентів. Запобігання інцидентам. Виявлення та аналіз. Вектори атаки. Ознаки події. Джерела прекурсорів та індикатори. Аналіз інцидентів. Документація про інцидент. Пріоритизація інцидентів. Повідомлення про інцидент. Стримування, викорінення та відновлення. Вибір стратегії стримування. Літ.: [13]; [14]	2

13	**Опрацьовування інциденту (частина 2)** Збір та обробка доказів. Ідентифікація атакуючих хостів. Викорінення та відновлення. Події після інциденту. Використання зібраних даних про інциденти. Зберігання доказів. Контрольний перелік обробки інцидентів. Літ.: [13]; [14]	2
14	**Координація та обмін інформацією** Координаційні відносини. Угоди про спільне використання та вимоги до звітності. Методи обміну інформацією (спеціальні, частково автоматизовані). Питання безпеки. Обмін детальною інформацією. Інформація про вплив на бізнес. Технічна інформація. Рекомендації. Літ.: [13]; [14]	2
Тема 5. Відновлення функціонування ІКС		
15	**Організаційно-технічні заходи відновлення функціонування ІКС** Аварія як можливий стан ІКС. Завдання аварійного планування та стадії відновлювальних робіт після аварії ІКС. Журнал аудиту подій. Літ.: [1] с. 119-127; [9]; [12]	2
16	**Резервування ресурсів ІКС та резервне зберігання даних** Вимоги до систем резервного копіювання. Види резервного копіювання. Схеми ротації. Методи боротьби з втратою даних. Політики резервного копіювання даних. Літ.: [2] с. 74-92; [11]	2
	Разом :	**32**

5.2 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	Розробка політики безпеки для корпоративної мережі підприємства	2
4	Оцінювання політики безпеки інформаційної системи підприємства на відповідність стандартам безпеки	2
5	Створення моделі управління інформаційною безпекою підприємства за допомогою програмного комплексу Coras	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. Тестування.	2
	Разом за семестр:	**18**

5.3 Зміст самостійної (у т.ч. індивідуальної) роботи

Самостійна робота студентів полягає у систематичному опрацюванні програмного матеріалу з відповідних джерел інформації, підготовці до виконання і захисту лабораторних робіт, підготовці до практичних занять, підготовці до тестування тощо. Керівництво самостійною роботою здійснюється викладачем згідно з розкладом консультацій у позаурочний час. Крім цього, до послуг студентів сторінка навчальної дисципліни у Модульному середовищі для навчання, де розміщені Робоча програма дисципліни та необхідні документи з її навчально-методичного забезпечення.

№ тижня	Теми самостійної роботи	Кількість годин
1	Опрацювання конспекту лекцій та теоретичного матеріалу лекції №1. Підготовка до практичного заняття №1.	6
2	Опрацювання конспекту лекцій та теоретичного матеріалу лекції №2. Виконання та здача практичного завдання №1.	6
3	Опрацювання конспекту лекцій та теоретичного матеріалу лекції №3. Підготовка до практичного заняття №2.	6
4	Опрацювання конспекту лекцій та теоретичного матеріалу лекції №4. Виконання та здача практичного завдання №2.	6
5	Опрацювання конспекту лекцій та теоретичного матеріалу лекції №5. Підготовка до практичного заняття №3.	6
6	Опрацювання конспекту лекцій та теоретичного матеріалу лекції №6. Виконання та здача практичного завдання №3.	6
7	Опрацювання конспекту лекцій та теоретичного матеріалу лекції №7. Підготовка до практичного заняття №4.	6
8	Опрацювання конспекту лекцій та теоретичного матеріалу лекції №8. Виконання та здача практичного завдання №4.	6

9	Опрацювання конспекту лекцій та теоретичного матеріалу лекції №9. Підготовка до практичного заняття №5.	6
10	Опрацювання конспекту лекцій та теоретичного матеріалу лекції №10. Виконання та здача практичного завдання №5.	6
11	Опрацювання конспекту лекцій та теоретичного матеріалу лекції №11. Підготовка до практичного заняття №6.	6
12	Опрацювання конспекту лекцій та теоретичного матеріалу лекції №12. Виконання та здача практичного завдання №6.	6
13	Опрацювання конспекту лекцій та теоретичного матеріалу лекції №13. Підготовка до практичного заняття №7.	6
14	Опрацювання конспекту лекцій та теоретичного матеріалу лекції №14. Виконання та здача практичного завдання №7.	6
15	Опрацювання конспекту лекцій та теоретичного матеріалу лекції №15. Підготовка до практичного заняття №8.	6
16	Опрацювання конспекту лекцій та теоретичного матеріалу лекції №16. Виконання та здача практичного завдання №8.	6
17	Підготовка до тестування за пройденим теоретичним матеріалом.	4
	Разом за семестр:	100

6. ТЕХНОЛОГІЇ ТА МЕТОДИ НАВЧАННЯ

Процес навчання з дисципліни ґрунтується на використанні традиційних та сучасних методів. Зокрема, лекції проводяться з використанням словесних, наочних та проблемних методів з супроводом презентаційних матеріалів; практичні заняття – з використанням практичних методів; самостійна робота (опрацювання теоретичного матеріалу, підготовка до виконання та захисту лабораторних робіт, тестування) – з використанням пояснювально-ілюстративних та дослідницьких методів, інформаційно-комп'ютерних технологій та технологій дистанційного навчання.

7. МЕТОДИ КОНТРОЛЮ

Поточний контроль здійснюється під час практичних занять. а також у дні проведення контрольних заходів, встановлених робочою програмою і графіком освітнього процесу, в т.ч. з використанням Модульного середовища для навчання. При цьому використовуються такі методи поточного контролю:

- тестовий контроль теоретичного матеріалу;
- оцінювання результатів виконання практичних завдань.

При виведенні підсумкової семестрової оцінки враховуються результати як поточного, так і підсумкового контролів, який проводиться з усього матеріалу дисципліни за білетами, попередньо розробленими і затвердженими на засіданні кафедри. Здобувач вищої освіти, який набрав з будь-якого виду навчальної роботи, суму балів нижчу за 60 відсотків від максимального балу, ***не допускається*** до семестрового контролю поки не виконає весь обсяг, передбачений Робочою програмою для цього виду роботи. Здобувач вищої освіти, який набрав позитивний середньозважений бал (60 відсотків і більше від максимального балу, встановленого для кожної структурної одиниці) з усіх видів поточного контролю і не склав іспит, вважається таким, який ***має*** академічну заборгованість. Ліквідація академічної заборгованості із семестрового контролю здійснюється у період екзаменаційної сесії або за графіком, встановленим деканатом відповідно до «Положення про контроль і оцінювання результатів навчання здобувачів вищої освіти у ХНУ».

8. ПОЛІТИКА ДИСЦИПЛІНИ

Політика навчальної дисципліни загалом визначається системою вимог до здобувача вищої освіти, що передбачені чинними положеннями Університету про організацію і навчально-методичне забезпечення освітнього процесу. Зокрема, проходження інструктажу з техніки безпеки; відвідування занять з дисципліни є обов'язковим. За об'єктивних причин (підтверджених документально) теоретичне навчання за погодженням із лектором може відбуватись в он-лайн режимі. Успішне опанування дисципліни і формування фахових компетентностей і програмних результатів навчання передбачає необхідність підготовки до практичних занять (вивчення теоретичного матеріалу з теми, активно працювати на занятті, розв'язувати задачі, брати участь у дискусіях щодо прийнятих рішень при виконанні здобувачами задач).

Здобувачі вищої освіти зобов'язані дотримуватися термінів виконання усіх видів робіт у встановлені терміни, передбачених робочою програмою навчальної дисципліни. Пропущене практичне заняття здобувач зобов'язаний відпрацювати в лабораторіях кафедри у встановлений викладачем термін, але не пізніше, ніж за два тижні до кінця теоретичних занять у семестрі.

Засвоєння здобувачем теоретичного матеріалу з дисципліни оцінюється за результатами тестування.

Здобувач вищої освіти, виконуючи практичні завдання, тестування з дисципліни, має дотримуватися політики доброчесності (заборонені списування, плагіат (в т.ч. із використанням мобільних девайсів)). У разі виявлення плагіату в будь-яких видах навчальної роботи здобувач вищої освіти отримує незадовільну оцінку і має повторно виконати завдання з відповідної теми (виду роботи), що передбачені робочою програмою. Будь-які форми порушення академічної доброчесності ***не допускаються.***

У межах вивчення навчальної дисципліни здобувачам вищої освіти передбачено визнання і зарахування результатів навчання, набутих шляхом неформальної освіти, що розміщені на доступних платформах (за наявності такого переліку, доцільно вказати рекомендовані курси), які сприяють формування компетентностей і поглибленню результатів навчання, визначених робочою програмою дисципліни, або забезпечують вивчення відповідної теми та/або виду робіт з програми навчальної дисципліни (детальніше у Положенні про порядок визнання та зарахування результатів навчання здобувачів вищої освіти у ХНУ).

9. ОЦІНЮВАННЯ РЕЗУЛЬТАТІВ НАВЧАННЯ ЗДОБУВАЧІВ ОСВІТИ

Оцінювання академічних досягнень здобувача вищої освіти здійснюється відповідно до «Положення про контроль і оцінювання результатів навчання здобувачів вищої освіти у ХНУ». Залежно від важливості окремих видів навчальної роботи, і їх ролі у формуванні компетентностей і результатів навчання, визначених освітньою програмою, розробники Робочої програми присвоюють кожному виду навчальної роботи (структурній одиниці) з дисципліни певну кількість балів. При поточному оцінюванні виконаної здобувачем роботи з кожної структурної одиниці і отриманих ним результатів викладач виставляє йому певну кількість балів із встановлених Робочою програмою для цього виду роботи. При цьому кожна структурна одиниця навчальної роботи може бути зарахована, якщо здобувач набрав не менше 60 відсотків (мінімальний рівень для позитивної оцінки) від максимально можливої суми балів, призначеної структурній одиниці.

Будь-які форми порушення академічної доброчесності ***не допускаються***.

При оцінюванні результатів навчання здобувачів вищої освіти з будь-якого виду навчальної роботи (структурної одиниці) рекомендується використовувати наведені нижче узагальнені критерії:

Таблиця – Критерії оцінювання навчальних досягнень здобувача вищої освіти

Оцінка та рівень досягнення здобувачем запланованих ПРН та сформованих компетентностей	**Узагальнений зміст критерія оцінювання**
Відмінно (високий)	Здобувач вищої освіти 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 мовою викладання (в усній або у письмовій формі), демонструє якісне оформлення роботи і володіння спеціальними приладами та інструментами, прикладними програмами. Здобувач не вагається при видозміні запитання, вміє робити детальні та узагальнюючі висновки, демонструє практичні навички з вирішення фахових завдань. При відповіді допустив дві–три несуттєві ***похибки***.
Добре (середній)	Здобувач вищої освіти виявив повне засвоєння навчального матеріалу, володіє понятійним апаратом, 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 правил, закономірностей тощо. Відповідь здобувача вищої освіти будується на основі самостійного мислення. Здобувач вищої освіти у відповіді допустив дві–три ***несуттєві помилки***.
Задовільно (достатній)	Здобувач вищої освіти 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 здобувача вищої освіти будується на рівні репродуктивного мислення, здобувач вищої освіти має слабкі знання структури навчальної дисципліни, 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 (недостатній)	Здобувач вищої освіти 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 здобувачеві вищої освіти, який не може продовжити навчання без додаткової роботи з вивчення навчальної дисципліни.

Структурування дисципліни за видами навчальної роботи і оцінювання результатів навчання здобувачів

Аудиторна робота								**Контрольні заходи**	**Семестровий контроль**	
Практичні заняття (мінімум 8 контрольних точок)								Тестовий контроль:	Іспит	Разом балів
1	2	3	4	5	6	7	8	Т1-5		
Кількість балів за вид навчальної роботи (мінімум-максимум)										
3-5	3-5	3-5	3-5	3-5	3-5	3-5	3-5	12-20	24-40	**60-100**
24-40								**12-20**	**24-40**	

Примітки: Т – тема навчальної дисципліни;

Оцінювання результатів виконання практичних завдань

Оцінка, яка виставляється за практичне заняття, складається з таких елементів: усне опитування на знання теоретичного матеріалу з теми; вільне володіння спеціальною термінологією і уміння професійно обґрунтувати прийняті рішення при розв'язуванні завдань; самостійність та правильність виконання.

Результат виконання кожного практичного завдання оцінюється відповідно до таблиці Критеріїв оцінювання навчальних досягнень здобувача вищої освіти та рівня досягнення здобувачем запланованих ПРН та сформованих компетентностей з присвоєнням йому відповідної суми балів.

Оцінювання результатів тестового контролю

Тест, передбачений робочою програмою, складається із 20 тестових завдань, кожне з яких є рівнозначним. Максимальна сума балів, яку може набрати здобувач, складає 20.

Відповідно до таблиці структурування видів робіт за тематичний контроль здобувач залежно від кількості правильних відповідей може отримати від 12 до 20 балів.

Розподіл балів в залежності від наданих правильних відповідей на тестові завдання

Кількість правильних відповідей	0-11	12	13	14	15	16	17	18	19	20
Відсоток правильних відповідей	0-59	60	65	70	75	80	85	90	95	100
Кількість отриманих балів	0	12	13	14	15	16	17	18	19	20

На тестування відводиться 20 хвилин. Правильні відповіді записуються у талоні відповідей. Здобувач може також пройти тестування і в он-лайн режимі у Модульному середовищі для навчання.

Оцінювання результатів підсумкового семестрового контролю (іспит)

Освітня програма передбачає підсумковий семестровий контроль з дисципліни у формі іспиту, завданням якого є системне й об'єктивне оцінювання підготовки здобувача з навчальної дисципліни. Складання іспиту відбувається за попередньо розробленими і затвердженими на засіданні кафедри білетами.

Таблиця – Оцінювання результатів підсумкового семестрового контролю здобувачів вищої освіти (40 балів для підсумкового контролю)

Види завдань	**Для кожного окремого виду завдань**		
	Мінімальний (достатній) бал (задовільно)	**Потенційні позитивні бали*** **(середній бал) (добре)**	**Максимальний (високий) бал (відмінно)**
Теоретичне питання № 1	6	8	10
Теоретичне питання № 2	6	8	10
Практичне завдання	12	16	20
Разом:	**24**		**40**

Примітка. ****Позитивний бал за іспит, відмінний від мінімального (24 бали) та максимального (40 балів), знаходиться в межах 25-39 балів та розраховується як сума балів за усі структурні елементи (завдання) іспиту.***

Для кожного окремого виду завдань підсумкового семестрового контролю застосовуються критерії оцінювання навчальних досягнень здобувача вищої освіти, наведені вище (**Таблиця – Критерії оцінювання навчальних досягнень здобувача вищої освіти)**.

Таблиця – Співвідношення інституційної шкали оцінювання і шкали оцінювання ЄКТС

Оцінка ЄКТС	**Рейтингова шкала балів**	**Інституційна шкала (Опис рівня досягнення здобувачем вищої освіти запланованих результатів навчання з навчальної дисципліни**	
		Залік	**Іспит/диференційований залік**
A	90-100	Зараховано	***Відмінно*/*Excellent*** – високий рівень досягнення запланованих результатів навчання з навчальної дисципліни, що свідчить про безумовну готовність здобувача до подальшого навчання та/або професійної діяльності за фахом
B	83-89		***Добре*/*Good*** – середній (максимально достатній) рівень досягнення запланованих результатів навчання з навчальної дисципліни та готовності до подальшого навчання та/або професійної діяльності за фахом
C	73-82		
D	66-72		***Задовільно*/*Satisfactory*** – Наявні мінімально достатні для подальшого навчання та/або професійної діяльності за фахом результати навчання з навчальної дисципліни
E	60-65		
FX	40-59	Незараховано	***Незадовільно*/*Fail*** – Низка запланованих результатів навчання з навчальної дисципліни відсутня. Рівень набутих результатів навчання є недостатнім для подальшого навчання та/або професійної діяльності за фахом
F	0-39		***Незадовільно*/*Fail*** – Результати навчання відсутні

Підсумкова семестрова оцінка за інституційною шкалою і шкалою ЄКТС визначається в автоматизованому режимі після внесення викладачем результатів оцінювання з усіх видів робіт до електронного журналу. Співвідношення інституційної шкали оцінювання і шкали оцінювання ЄКТС у наведеній вище таблиці.

Семестровий іспит виставляється, якщо загальна сума балів, яку набрав здобувач з дисципліни за результатами поточного та підсумкового контролю, знаходиться у межах від 60 до 100 балів. При цьому за інституційною шкалою ставиться оцінка «відмінно/добре/задовільно», а за шкалою ЄКТС – буквене позначення оцінки, що відповідає набраній здобувачем сумі балів відповідно до таблиці Співвідношення.

10. ПИТАННЯ ДЛЯ САМОКОНТРОЛЮ 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. Джерела інформації про події та типи подій.
19. Види та застосування систем SIEM.
20. Принцип роботи системи SIEM.
21. Приклади комерційних систем SIEM.
22. Створення політики, плану та процедур реагування на інциденти.
23. Структура групи реагування на інциденти.
24. Моделі команд. Вибір моделі команди.
25. Персонал реагування на інциденти. Залежності всередині організацій.
26. Життєвий цикл атаки (Kill Chain).
27. Опрацьовування інциденту.
28. Координаційні відносини. Угоди про спільне використання та вимоги до звітності.
29. Методи обміну інформацією (спеціальні, частково автоматизовані).
30. Аспекти ІБ при управлінні безперервністю бізнесу.
31. Аварія як можливий стан ІКС.
32. Завдання аварійного планування та стадії відновлювальних робіт після аварії ІКС.
33. Журнал аудиту подій.
34. Вимоги до систем резервного копіювання.
35. Види резервного копіювання.
36. Схеми ротації. Методи боротьби з втратою даних.
37. Політики резервного копіювання даних.
38. Основи та поняття СУІБ.
39. Сфера застосування СУІБ.
40. Терміни та визначення СУІБ.
41. Сертифікація СУІБ.
42. Вимоги до СУІБ.
43. Цілі і засоби СУІБ.
44. Визначення області дії, меж і політики СУІБ.
45. Проведення аналізу вимог до ІБ.
46. Основні процеси розробки СУІБ.
47. Проведення аналізу вимог до ІБ.
48. Надання послуг в сфері інформаційної безпеки.
49. Програмна підтримка роботи з політикою безпеки.
50. Програмні засоби, що інтегруються в СУІБ підприємства.
51. Аудит стану інформаційної безпеки на підприємстві.
52. Модель СУІБ підприємства.
53. Етапність аудиту інформаційної безпеки.
54. Оцінка відповідності ІС вимогам стандартів.
55. Методика аналізу захищеності інформаційних активів.
56. Передумови розвитку менеджменту в сфері інформаційної безпеки.
57. Загальна структура управлінської роботи по забезпеченню інформаційної безпеки на підприємстві.
58. Віднесення відомостей до комерційної таємниці.
59. Віднесення відомостей до державної таємниці.
60. Організація доступу до таємної інформації.
61. Захист службової інформації.
62. Адміністративний рівень управління ІБ.
63. Процедурний рівень управління ІБ.
64. Реагування на порушення режиму безпеки.
65. Планування відновлювальних робіт.
66. Права працівників на доступ до серверів і баз даних колективного використання.
67. Департамент інформаційної безпеки.
68. Планування персоналу.
50. Етапи формування трудового колективу.

11. МЕТОДИЧНЕ ЗАБЕЗПЕЧЕННЯ

Освітній процес з дисципліни «Управління інформаційною безпекою» забезпечений необхідними навчально-методичними матеріалами, що розміщені в Модульному середовищі для навчання MOODLE:

1. Курс «Управління інформаційною безпекою»: https://msn.khmnu.edu.ua/course/view.php?id=6792.

12. МАТЕРІАЛЬНО-ТЕХНІЧНЕ ТА ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ

Інформаційна та комп'ютерна підтримка: ПК, ноутбук, планшет, смартфон або інший мобільний пристрій, проєктор, доступ до мережі Інтернет, робота з презентаціями.

Спеціальне та прикладне програмне забезпечення: OS Kali Linux, OS Ubuntu, OS MS Windows 10 або вище, Oracle Virtual Box, Ettercap, Wireshark, Nessus, Snort/Suricata, Nmap (Zenmap), MS Visual Studio 19 або вище, Docker, MISP Threat Sharing, CORAS Tools тощо.

13. РЕКОМЕНДОВАНА ЛІТЕРАТУРА

Основна

1. Комплексна безпека інформаційних мережевих систем: навчальний посібник/ Укладачі: А.Г. Микитишин, М.М. Митник, О.С. Голотенко, В.В. Карташов. Тернопіль: ФОП Паляниця В.А., 2023. – 324 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. Information Security Handbook/ Noor Zaman Jhanjhi, Khalid Hussain, Mamoona Humayun, Azween Bin Abdullah, João Manuel R.S. Tavares. CRC Press, 2022. 250 p.
4. 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.
5. Інформаційні мережі: навчальний посібник / Ю. В. Коваль, А. Б. Ставровський. Київ, 2021. 84 с.

Додаткова

6. NIST SP 800-30. Guide for Conducting Risk Assessments.
7. ISO/IEC 27005. Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки.
8. ISO/IEC 27000. Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Огляд та словник термінів.
9. ISO/IEC 27001. Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою.
10. ISO/IEC 27003. Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Керівництво.
11. ISO/IEC 27002. Інформаційні технології. Методи захисту. Звід правил для управління інформаційною безпекою.
12. ISO/IEC 15408. Інформаційні технології. Кібербезпека та захист конфіденційності. Критерії оцінювання безпеки ІТ.
13. ISO/IEC 13335. Інформаційні технології. Настанови з керування безпекою інформаційних технологій (ІТ)
14. NIST SP 800-61. Computer Security Incident Handling Guide.
15. ISO/IEC 27035. Інформаційні технології. Методи захисту. Керування інцидентами інформаційної безпеки.
16. CISA Посібник з додаткових ресурсів CRR. Том 5. Управління кіберінцидентами.
17. Kali Docs [Електронний ресурс]. Режим доступу: https://www.kali.org/docs/
18. Kali Tools [Електронний ресурс]. Режим доступу: https://www.kali.org/tools/
19. Snort. Documents [Електронний ресурс]. Режим доступу: https://www.snort.org/documents
20. Suricata [Електронний ресурс]. Режим доступу: https://suricata.io
21. Інструменти для аналізу шкідників. Інструменти динамічного аналізу та пісочниці [Електронний ресурс]. Режим доступу: https://surl.li/bunfov
22. Що таке платформа MISP і як нею користуватися? [Електронний ресурс]. Режим доступу: https://kr-labs.com.ua/blog/shcho-take-platforma-misp
23. CORAS A risk modeling approach [Електронний ресурс]. Режим доступу: https://coras.tools/#/try-it
24. Методика ідентифікації та оцінювання важливості інформаційних активів/ Віра Тітова, Юрій Кльоц, Богдан Кальчун, Анна Кувіла, Ірина Рак// Вісник Хмельницького національного університету, 2024. №5. С. 521-525
25. Розроблення політики інформаційної безпеки приватного підприємства/ В. Тітова, Ю. Кльоц, В. Волинець, Н. Петляк, М. Огородник// Measuring and computing devices in technological processes, 2024. С. 79-83
26. Порівняльний аналіз моделей атак на інформаційну безпеку/ В. Тітова, Ю. Кльоц, З. Лакоценін, О. Шлапак, В. Троц// Вісник Хмельницького національного університету, 2024.
27. Fuzzy inference subsystem for classifying threats to computer information/ Віра Тітова, Юрій Кльоц, Наталія Петляк, Марія Капустян// Measuring and computing devices in technological processes, 2022. №1. С. 57-61.
28. Detection of network attacks in cyber-physical systems using a rule-based logical neural network/ Titova, V., Klots, Y., Cheshun, V., Petliak, N., Salem, A.-B.M.// CEUR Workshop, 2024, 3736, P. 255–268
29. 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, P. 378–389

14. ІНФОРМАЦІЙНІ РЕСУРСИ

1. Модульне середовище для навчання. URL : https://msn.khmnu.edu.ua/course/view.php?id=6792
2. Електронна бібліотека ХНУ. URL: http://lib.khmnu.edu.ua/
3. Інституційний репозитарій ХНУ. URL : https://library.khmnu.edu.ua/

УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

Тип дисципліни	Обов'язкова
Рівень вищої освіти	Перший (бакалаврський)
Мова викладання	Українська
Семестр	Сьомий
Кількість встановлених кредитів ЄКТС	5
Форми здобуття освіти, для яких викладається дисципліна	Очна (денна)

Результати навчання. Після вивчення дисципліни студент повинен: *виявляти*, *формулювати* та *вирішувати* проблеми в управлінні інформаційною безпекою, *організовувати* професійну діяльність, *планувати* неперервність бізнесу згідно з політикою безпеки та стандартами; самостійно *застосовувати* законодавчу й нормативну базу, *розслідувати* інциденти, *приймати* обґрунтовані рішення в складних умовах, *оцінювати* їхню ефективність; *здійснювати* управління інцидентами кібербезпеки, *автоматизувати* процеси моніторингу подій, *використовувати* сучасні моделі безпеки для керування доступом, *розробляти* стратегії кіберзахисту, *впроваджувати* політики, *готувати* нормативні пропозиції, *проводити* атестацію об'єктів; *відновлювати* роботу систем після інцидентів, *застосовувати* сучасні ІКТ і *прогнозувати* результати управління.

Зміст навчальної дисципліни. Основи управління ІБ. Правила управління ІБ. Політики інформаційної безпеки. Системи управління інформаційною безпекою (СУІБ). Основи та поняття СУІБ. Вимоги до СУІБ. Розробка СУІБ. Моніторинг ІБ та SIEM. Розуміння інцидентів кібербезпеки. Організація реагування та розслідування кіберінцидентів. Структура групи реагування на інциденти. Життєвий цикл атаки (Kill Chain). Опрацьовування інциденту. Координація та обмін інформацією. Відновлення функціонування ІКС. Організаційно-технічні заходи відновлення функціонування ІКС. Резервування ресурсів ІКС та резервне зберігання даних.

Пререквізити: нормативно-правове забезпечення кібербезпеки.

Постреквізити: комплексні системи захисту інформації, переддипломна практика.

Запланована навчальна діяльність: Мінімальний обсяг навчальних занять в одному кредиті ЄКТС навчальної дисципліни для першого (бакалаврського) рівня вищої освіти за денною формою здобуття освіти становить 10 годин на 1 кредит ЄКТС.

Форми (методи) навчання: лекції (з використанням словесних, наочних та проблемних методів з супроводом презентаційних матеріалів); практичні заняття (з використанням практичних методів); самостійна робота (з використанням пояснювально-ілюстративних та дослідницьких методів).

Форми оцінювання результатів навчання: оцінювання на практичних заняттях; тестовий контроль; оцінювання результатів підсумкового семестрового контролю (іспит).

Вид семестрового контролю: іспит.

Навчальні ресурси:

1. Комплексна безпека інформаційних мережевих систем: навчальний посібник/ Укладачі: А.Г. Микитишин, М.М. Митник, О.С. Голотенко, В.В. Карташов. Тернопіль: ФОП Паляниця В.А., 2023. 324 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. Information Security Handbook/ Noor Zaman Jhanjhi, Khalid Hussain, Mamoona Humayun, Azween Bin Abdullah, João Manuel R.S. Tavares. CRC Press, 2022. 250 p.
4. 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.
5. Інформаційні мережі: навчальний посібник / Ю. В. Коваль, А. Б. Ставровський. Київ, 2021. 84 с.
6. Модульне середовище для навчання. Доступ до ресурсу: https://msn.khmnu.edu.ua/course/view.php?id=6792
7. Електронна бібліотека університету. Доступ до ресурсу: http://lib.khmnu.edu.ua

Викладач: канд. техн. наук, доцент Віра Тітова.