ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет програмування та комп'ютерних і телекомунікаційних систем
Кафедра кібербезпеки та комп'ютерних систем і мереж

ЗАТВЕРДЖУЮ
Декан ФПКТС
_____ Савенко О.С.
підпис
«22» січня 2021 р.

СИЛАБУС
Навчальна дисципліна: "Управління інформаційною безпекою"

Освітньо-професійна програма: «Кібербезпека»

Рівень вищої освіти: перший (бакалаврський)

Загальна інформація

Позиція	Інформація
Викладач(і)	Молодецька Катерина Валеріївна
Профайл викладач(ів)	http://ksm.khnu.km.ua/sklad-kafedry/
E-mail викладача(ів)	kksmkhnu@gmail.com
Контактний телефон	Наявний в ІСУ
Сторінка дисципліни в ІСУ	https://msn.khnu.km.ua/enrol/index.php?id=6792
Сторінки інтернет-ресурсів для онлайн занять	ZOOM: https://us04web.zoom.us/j/521227760 * пароль у викладача, старости групи і на сторінці дисципліни в ІСУ
Навчальний рік, семестр	2022-2023, семестр VII (осінньо-зимовий)
Розклад	
Консультації	

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
Д	4	7	5	150	51	34	-	17	-	99	-	-	-	+

Анотація дисципліни

Дисципліна викладається для студентів денної форми навчання спеціальності «Кібербезпека». При викладанні дисципліни використовуються наступні форми (методи) навчання: пояснювально-ілюстративні, практичні, продуктивні, проблемні, контекстні, тренінгові, застосування інформаційно-комп'ютерних технологій (MS Security Assessment Tool, IBM Qradar та інших).

Пререквізити: стандарти і політики кібербезпеки, кібернетичне право.

Кореквізити: переддипломна практика

Мета і завдання дисципліни

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.

Тематичний і календарний план вивчення дисципліни

№ тижня	Тема лекції*	Тема практ. роботи**	Самостійна роботи		
			Зміст	Год.	Література
1	**Основи управління інформаційною безпекою (ІБ).** Поняття та термінологія управління ІБ. Об’єкти та складові управління ІБ. Важливість і складність проблем управління ІБ	-	Опрацювання теоретичного матеріалу лекції №1.	5	[1] с. 8-30 [3] с. 19-38 [4] с. 1-74
2	**Правила управління інформаційною безпекою (частина 1).** Організація ІБ. Безпека, пов'язана з персоналом. Управління активами	**ПЗ №1** Ідентифікація та оцінювання інформаційних активів підприємства	Опрацювання теоретичного матеріалу лекції №2. Виконання завдань ПЗ №1.	5	[2] с. 60-71 [6] с. 1-29 [17] с. 240-295
3	**Правила управління інформаційною безпекою (частина 2).** Управління доступом. Криптографія в задачах управління ІБ. Фізична та екологічна безпека	-	Опрацювання теоретичного матеріалу лекції №3.	6	[6] с. 29-37, с. 60-77, с. 80-83 [17] с. 295-324

4	**Правила управління інформаційною безпекою (частина 3).** Безпека операцій. Безпека зв'язку	**ПЗ №2** Ідентифікація загроз інформаційним активам підприємства та їх джерел	Опрацювання теоретичного матеріалу лекції №4. Виконання завдань ПЗ №2.	6	[2] с. 60-71 [6] с. 37-60 [7] с. 22-35 [17] с. 324-345
5	**Правила управління інформаційною безпекою (частина 4).** Придбання, розробка, впровадження та супровід інформаційних систем (ІС). Взаємовідносини з постачальниками	-	Опрацювання теоретичного матеріалу лекції №5.	6	[6] с. 77-90 [17] с. 345-364
6	**Управління інцидентами інформаційної безпеки.** Виявлення інцидентів ІБ. Реєстрація інцидентів, ведення журналів реєстрації. Реагування на інциденти. Розслідування та збір правових доказів. Аспекти ІБ при організації безперервності бізнесу	**ПЗ №3** Оцінювання інформаційної системи підприємства на відповідність стандартам безпеки	Опрацювання теоретичного матеріалу лекції №6. Виконання завдань ПЗ №3.	6	[1] с. 105-118 [6] с. 90-107 [17] с. 364-373
7	**Основи та поняття систем управління інформаційною безпекою (СУІБ).** Сфера застосування СУІБ. Терміни та визначення СУІБ. Сертифікація СУІБ	-	Опрацювання теоретичного матеріалу лекції №7.	6	[8] с. 1-26 [17] с. 71-83
8	**Вимоги до систем управління інформаційною безпекою.** Планування СУІБ. Експлуатація СУІБ. Оцінка результативності СУІБ. Вдосконалення СУІБ	**ПЗ №4** Створення моделі системи управління інформаційною безпекою підприємства	Опрацювання теоретичного матеріалу лекції №8. Виконання завдань ПЗ №4.	6	[5] с. 1-23 [7] с. 10-17 [17] с. 83-127

9	**Розробка систем управління інформаційною безпекою.** Визначення області дії, меж і політики СУІБ. Проведення аналізу вимог до ІБ. Проведення оцінювання і планування обробки ризиків. Основні процеси розробки СУІБ	-	Опрацювання теоретичного матеріалу лекції №9.	6	[9] с. 1-45
10	**Аудит інформаційної безпеки підприємства.** Поняття аудиту безпеки і мети його проведення. Етапність аудиту. Оцінка відповідності вимогам стандарту. Ризик-менеджмент. Вироблення рекомендацій та підготовка звітної документації. Методика аналізу захищеності	**ПЗ №5** Збір та систематизація технічної інформації при підготовці аудиту інформаційної безпеки підприємства	Опрацювання теоретичного матеріалу лекції №10. Виконання завдань ПЗ №5.	6	[1] с. 119-127 [10] с. 7-33 [11] с. 21-31 [17] с. 383-407
11	**Організація секретного діловодства.** Віднесення відомостей до комерційної таємниці. Віднесення відомостей до державної таємниці. Організація доступу до таємної інформації. Захист службової інформації	-	Опрацювання теоретичного матеріалу лекції №11.	6	[2] с. 74-92 [15] с. 24-38
12	**Адміністративний та процедурний рівні управління інформаційною безпекою.** Матриця управління доступом та розподіл інформаційних потоків. Моделі та політики управління доступом (мандатні, дискреційні, рольові). Фізичний захист та підтримка працездатності. Реагування на порушення режиму безпеки. Планування відновлювальних робіт	**ПЗ №6 та №7** Проведення аудиту інформаційної безпеки підприємства	Опрацювання теоретичного матеріалу лекції №12. Виконання завдань ПЗ №6 та №7.	7	[2] с. 114-123 [11] с. 31-36, с. 42-48 [12] с. 55-95

13	**Основи роботи з персоналом.** Планування персоналу. Етапи формування трудового колективу. Підбір і розстановка персоналу. Особливості відбору співробітників, які допускаються до роботи з конфіденційною інформацією	-	Опрацювання теоретичного матеріалу лекції №13.	6	[13] с. 47-60 [14] с. 52-122 [18] с. 4-24 [19] с. 1-65
14	**Апаратно-програмні засоби захисту інформації в задачах управління ІБ.** Види та застосування систем SIEM. Принцип роботи системи SIEM. Приклади комерційних систем SIEM. QRadar від IBM. Принципи роботи міжмережевих екранів	**ПЗ №8** Дослідження подій та інцидентів на підприємстві, ведення журналів реєстрації	Опрацювання теоретичного матеріалу лекції №14. Виконання завдань ПЗ №8.	7	[13] с. 47-60 [14] с. 74-122 [18] с. 17-21 [19] с. 1-65
15	**Інформаційна безпека України.** Забезпечення ІБ України. Система та політика забезпечення ІБ. України ІБ України у сфері прав і свобод людини	-	Опрацювання теоретичного матеріалу лекції №15.	6	[2] с. 124-163
16	**Організаційно-правові аспекти національної безпеки України.** Основні напрями державної політики з питань НБ України. Місце і роль ІБ в системі НБ держави	**Контрольна робота**	Опрацювання теоретичного матеріалу лекції №16. Підготовка до контрольної роботи.	6	[12] с. 8-55 [15] с. 38-56, с. 85-92
17	**Організаційно-правові аспекти забезпечення безпеки і стійкості критичної інфраструктури України.** Система безпеки та стійкості критичної інфраструктури. Методологічні та організаційні засади забезпечення безпеки та стійкості критичної інфраструктури	-	Опрацювання теоретичного матеріалу лекції №17.	4	[16] с. 11-31, с. 87-164

*** лекції проводяться по 2 години щотижня;**

**** практичні проводяться по 2 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, практичні заняття згідно з розкладом, не запізнюватися на заняття, вчасно виконувати та здавати практичні завдання. Термін виконання практичного завдання вважається своєчасним, якщо студент здав його на поточному або наступному за ним занятті. За несвоєчасний захист з набраної студентом суми балів вираховується один бал. Пропущене з поважної причини практичне заняття студент повинен відпрацювати у встановлений викладачем термін.

Набуті особою знання з дисципліни або її окремих розділів у неформальній освіті зараховуються відповідно до Положення про порядок перезарахування результатів навчання та визначення академічної різниці у ХНУ https://www.khnu.km.ua/root/files/01/10/03/006.pdf.

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	1-3	1-4	1-4
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

№	Назва	Режим доступу
1.	Основи інформаційної безпеки. Конспект лекцій./ Б.А. Заплотинський. – КІПВіП НУ "ОЮА", кафедра інформаційно-аналітичної та інноваційної діяльності, 2017. – 128 с.	http://dspace.onua.edu.ua/bitstream/handle/11300/11111/ОІБ%20конспект%20лекцій.pdf?sequence=1&isAllowed=y
2.	Інформаційна безпека держави: навч. посіб./ В.І. Гур'єв, Д.Б. Мехед, Ю.М. Ткач, І.В. Фірсова. – Ніжин: ФОП Лук'яненко В.В. ТПК «Орхідея», 2018. – 166 с.	http://ir.stu.cn.ua/bitstream/handle/123456789/19246/Інформ.%20безпека%20держ.%20New%20booklet%201.pdf?sequence=1&isAllowed=y
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.	https://drive.google.com/file/d/1Zqzz0pxqtm8KfmDnUvqYRWDYi0o6qsR_/view?usp=sharing
4.	ISO/IEC 15408. Information technology – Security techniques – Evaluation criteria for IT security – Part 1: Introduction and general model. – ISO: Geneva, 2009. – 74 p.	https://standards.iso.org/ittf/PubliclyAvailableStandards/index.html
5.	ISO/IEC 27001:2013. Information technology – Security techniques – Information security management systems – Requirements. – ISO: Geneva, 2013. – 32 p.	https://trofisecurity.com/assets/img/iso27001-2013.pdf
6.	ISO/IEC 27002:2013. Information technology – Security techniques – Code of practice for information security management. – ISO: Geneva, 2013. – 136 p.	http://bcc.portal.gov.bd/sites/default/files/files/bcc.portal.gov.bd/page/adeaf3e5_cc55_4222_8767_f26bcaec3f70/ISO_IEC_27002.pdf
7.	Методичні вказівки до виконання практичних робіт з навчальної дисципліни "Менеджмент інформаційної безпеки"/ І. А. Лисенко – Кропивницький: ЦНТУ, 2018.– 64 с.	http://dspace.kntu.kr.ua/jspui/bitstream/123456789/8431/1/Osn_ypr_kiber.pdf
8.	ISO/IEC 27000:2018. Information technology – Security techniques – Information security management systems – Overview and vocabulary. – ISO: Geneva, 2018. – 34 p.	https://akela.mendelu.cz/~lidak/IPI/ISO_IEC_27000_2018.pdf
9.	ISO/IEC 27003:2017. Information technology – Security techniques – Information security management systems – Guidance. – ISO: Geneva, 2017. – 76 p.	https://drive.google.com/file/d/1Sa0qF50r7WkneMLpdfxFrlvxS4IRGEax/view?usp=sharing
10.	Аудит та управління інцидентами інформаційної безпеки : навч. посіб. / Корченко О.Г., Гнатюк С.О., Казмірчук С.В. та ін. – К. : Центр навч.-наук. та наук.-пр. видань НА СБ України, 2014. – 190 с.	https://er.nau.edu.ua/bitstream/NAU/38027/1/Audit%26Incident_15042014.pdf
11.	Інформаційна безпека держави: методичні вказівки до виконання лабораторних робіт / уклад. О.А. Смірнов, О.К. Конопліцька-Слободенюк, В.Д. Хох, С.А. Смірнов/ –	http://dspace.kntu.kr.ua/jspui/bitstream/123456789/8231/1/Inform_bezpeka_derjavu.PDF

	Кропивницький: ЦНТУ – 2017. – 90 с.	
12.	Інформаційна безпека: питання правового регулювання: монографія / А.Ю. Нашинець-Наумова. – Київ: Видавничий дім «Гельветика», 2017. – 168 с.	http://elibrary.kubg.edu.ua/id/eprint/18860/1/A_Nashinets-Naumova_monografia_1_FPMV.pdf
13.	Економічна безпека підприємства: навчальний посібник [Електронний ресурс]/ Небава М. І., Міронова Ю.В. – Вінниця: ВНТУ, 2017.	https://web.posibnyky.vntu.edu.ua/fmib/33nebava_ekonomichna_bezpeka_pidpriyemstva/ekon_bezp_Nebava.pdf
14.	Управління персоналом : курс лекцій / Н.С. Іванова – Кривий Ріг: ДонНУЕТ, 2017.– 140 с.	http://elibrary.donnuet.edu.ua/1390/1/Ivanova_Konspekt%20lektsiy_Upravlinnia_personalom.pdf
15.	Інформаційна безпека держави: навчальний посібник/ Т.М.Мужанова. – К.: ДУТ, 2019. – 131 с.	http://www.dut.edu.ua/uploads/l_1856_97597210.pdf
16.	Організаційні та правові аспекти забезпечення безпеки і стійкості критичної інфраструктури України : аналітична доповідь/ Д.Г. Бобро, С.П. Іванюта, С.І. Кондратов, О.М. Суходоля/ за заг. ред. О. М. Суходолі. – К.: НІСД, 2019. – 224 с.	https://niss.gov.ua/sites/default/files/2019-05/Dopov_Suchodolya_print.pdf
17.	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.	http://ir.stu.cn.ua/bitstream/handle/123456789/19244/Менеджмент%20інформ.%20безп.%20New%20booklet%201.pdf?sequence=1&isAllowed=y
18.	Апаратно-програмні засоби захисту інформації у корпораціях: навчально-методичний посібник [Електронний ресурс]/ В.Г. Крижановський, С.П. Сергієнко. – Вінниця : ДонНУ імені Василя Стуса, 2019.	https://r.donnu.edu.ua/bitstream/123456789/111/1/Методичка%20Засоби%20захисту%20інформації%20у%20корпораціях.pdf
19.	IBM QRadar. Installation Guide [Електронний ресурс]. – IBM Corp., 2019.	https://www.ibm.com/support/knowledgecenter/SS42VS_7.3.3/com.ibm.qradar.doc/b_siem_inst.pdf

Додаткова

20.	Information Security Management Handbook, Sixth Edition/ Micki Krause Nozaki, Harold F. Tipton. - CRC Press, 2011. – 458 p.	https://www.pdfdrive.com/information-security-management-handbook-d39563803.html
21.	Practical Information Security Management: A Complete Guide to Planning and Implementation/ Tony Campbell. – Australia: Burns Beach, 2016. – 253 p.	http://www.dut.edu.ua/ru/lib/1/category/742/view/1888
22.	Cyber-Development, Cyber-Democracy and Cyber-Defense: Challenges, Opportunities and Implications for Theory, Policy and Practice/ E. G. Carayannis, D. F. J. Campbell, M. P.s Efthymiopoulos. – New York: Springer, 2014. – 360 p.	https://kr.b-ok.as/book/2464958/0bd77c
23.	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.	https://pdfs.semanticscholar.org/6653/6d70cf96b5a7a45edbb35d001c7917db9959.pdf
24.	An integrated conceptual model for information system security risk management supported by enterprise architecture management/ N.	http://www.nmayer.eu/publis/Mayer%20et%20al.%20-%20SoSyM18.pdf

	Mayer, J. Aubert, E. Grandry, C. Feltus, E. Goettelmann, R. Wieringa [електронний ресурс]. – Software & Systems Modeling, 2018.	
25.	Управління інформаційною безпекою держави та підприємств: правові та організаційні аспекти/ В. Панченко. – Актуальні проблеми правознавства. – 2020. – 1 (21). – С. 103-109.	http://appj.tneu.edu.ua/index.php/appj/article/view/938/926
26.	Удосконалення системи управління інформаційною безпекою на підприємстві/ Ю.О. Русіна, В.Ю. Острякова. – Международный научный журнал «Интернаука». – 2017. – № 14 (36). – С. 135-139.	http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?I21DBN=LINK&P21DBN=UJRN&Z21ID=&S21REF=10&S21CNR=20&S21STN=1&S21FMT=ASP_meta&C21COM=S&2_S21P03=FILA=&2_S21STR=mnj_2017_14_29
27.	Методологія побудови системи забезпечення інформаційної безпеки банківської інформації в автоматизованих банківських системах/ Р.В. Грищук, С. П. Євсеєв. – Ukrainian Scientific Journal of Information Security. – 2017. – № 23, ч.3. – С. 204-214.	http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?I21DBN=LINK&P21DBN=UJRN&Z21ID=&S21REF=10&S21CNR=20&S21STN=1&S21FMT=ASP_meta&C21COM=S&2_S21P03=FILA=&2_S21STR=bezin_2017_23_3_9
28.	Система забезпечення кібербезпеки: сутність та призначення/ І. Діордіца. – Інформаційне право. – 2017. – №7. – С. 109-116.	http://www.pgp-journal.kiev.ua/archive/2017/7/24.pdf
29.	Оцінювання стану інформаційної безпеки підприємства/ А.В. Велігура. – Управління проектами та розвиток виробництва. – 2014. – №4 (52) – С. 28-39.	https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwjlvrOl2NTrAhWplYsKHc-HBFwQFjAFegQIBBAB&url=http%3A%2F%2Fwww.irbis-nbuv.gov.ua%2Fcgi-bin%2Firbis_nbuv%2Fcgiirbis_64.exe%3FC21COM%3D2%26I21DBN%3DUJRN%26P21DBN%3DUJRN%26IMAGE_FILE_DOWNLOAD%3D1%26Image_file_name%3DPDF%2FUprv_2014_4_6.pdf&usg=AOvVaw1ugYo4j_Yv5hUArkgfQKMF
30.	Соціальні інтернет-сервіси як суб'єкт інформаційної безпеки держави/ К. Молодецька. – Інформаційні технології та безпека. – 2016, №4, т.1. – С. 13-20.	https://ela.kpi.ua/bitstream/123456789/21431/1/ITS2016.4.1(6)-02.pdf
31.	Виявлення загроз інформаційній безпеці держави у змісті текстового контенту соціальних інтернет-сервісів/ О.В. Барабаш, Р. В. Грищук, К. В. Молодецька-Гринчук. – Наукоємні технології № 2(38), 2018. – С. 232-239.	http://jrnl.nau.edu.ua/index.php/SBT/article/view/12855
32.	Методологія побудови системи забезпечення інформаційної безпеки держави у соціальних інтернет-сервісах/ Р. Грищук, К. Молодецька-Гринчук. – Захист інформації. - 2017. - Т. 19, № 4. - С. 254-262.	http://nbuv.gov.ua/UJRN/Zi_2017_19_4_3

ІНФОРМАЦІЙНІ РЕСУРСИ:

1. Модульне середовище для навчання (розміщені усі необхідні матеріали з дисципліни, в тому числі завдання для поточного та семестрового контролю знань). Доступ до ресурсу: https://msn.khnu.km.ua.
2. Електронна бібліотека університету. Доступ до ресурсу: http://lib.khnu.km.ua/asp/php_f/p1age_lib.php.

Розробник _____ д.т.н., професор _____ К.В. Молодецька
Підпис Вчений ступінь, звання Ініціали, прізвище викладача(ів)

Погоджено
Гарант освітньої програми _____ к.т.н., доцент _____ В.М. Чешун
Підпис Вчений ступінь, звання Ініціали, прізвище

Зав. кафедри кібербезпеки та
комп'ютерних систем і мереж _____ к.т.н., доцент _____ Ю.П. Кльоц
Підпис Вчений ступінь, звання Ініціали, прізвище