ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

ЗАТВЕРДЖУЮ
Декан факультету ІТ
_____ Олег САВЕНКО
Підпис Ім'я, ПРІЗВИЩЕ
«31» 08 2023 р.

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Нормативно-правове забезпечення кібербезпеки

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.10
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)	3	5	5	150	68	34			34	82				+

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. Віктор ЧЕШУН
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

НОРМАТИВНО-ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ

Тип дисципліни Обов'язкова
Рівень вищої освіти Перший (бакалаврський)
Мова викладання Українська
Семестр П'ятий
Кредити ЄКТС 5,0
Форми навчання, для яких викладається дисципліна Денна очна

Студент, який успішно завершив вивчення дисципліни, повинен: *застосовувати* набуті знання для розуміння предметної області та розуміння професії, *критично осмислювати* основні теорії, принципи, методи і поняття у навчанні та професійній діяльності; *приймати участь* у розробці, впровадженні та оцінці стратегії і політик інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації із застосуванням різних класів політик інформаційної безпеки та/або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів, сучасних принципах, способах та методах теорії захищених систем; *виконувати* пошук, оброблення, аналіз та синтез інформації з різних джерел інформації (державних та міжнародних стандартів тощо) для ефективного рішення спеціалізованих задач професійної діяльності; *застосовувати* державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі інформаційної та/або кібербезпеки на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів і для підготовки пропозицій до нормативних актів щодо забезпечення інформаційної та/або кібербезпеки; *застосовувати* здобуті знання міжнародних та національних стандартів, сучасних методів і моделей політик інформаційної безпеки та/або кібербезпеки, розуміння принципів і навички синтезу на їх основі політик безпеки для вирішення задач управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових); *застосовувати* знання державної та іноземних мов для вивчення міжнародних та національних стандартів, а також *використовувати* термінологію цих стандартів з метою забезпечення ефективності професійної комунікації.

Зміст навчальної дисципліни. Концепція, стратегія та політики інформаційної безпеки; методи синтезу і аналізу політик безпеки; мандатна, дискреційна і рольова моделі політик безпеки; багаторівнева організація політики безпеки; політики безпеки провідних фірм в галузі інформаційних систем і технологій; міжнародні та національні стандарти інформаційної безпеки (ITSEC, FCITS, CTCPEC, BSI, BS, ISO, IEC, МЕК, ДСТУ тощо), їх вимоги та правила застосування.

Пререквізити: основи інформаційної безпеки; англійська мова.

Кореквізити: мережеві операційні системи; захист інформації в інформаційно-комунікаційних системах; управління інформаційною безпекою.

Запланована навчальна діяльність: лекції 34 год., практичних (семінарських) занять 34 год., самостійної роботи 82 год., разом 150 год.

Форми (методи) навчання: пояснювально-ілюстративні, практичні, продуктивні та репродуктивні, тренінгові, розвитку критичного мислення, застосування інформаційно-комп'ютерних технологій.

Форми оцінювання результатів навчання: усне опитування, практична перевірка (ділові ігри, презентації), тестування.

Вид семестрового контролю: іспит.

Навчальні ресурси:

1. Законодавство України. Офіційний портал Верховної Ради України. https://zakon.rada.gov.ua/laws
2. ISO Standards. Офіційний портал ISO – International Organization for Standardization. https://www.iso.org/standards.html
3. Гулак Г.М. Методологія захисту інформації. Аспекти кібербезпеки: підручник. К.: Видавництво НА СБ України, 2020. 256с.
4. Даник Ю.Г., Воробієнко П. П., Чернега В. М. Основи кібербезпеки та кібероборони: підручник / Видання друге, перероб. та доп. Одеса : ОНАЗ ім. О.С. Попова, 2019. 320 с.
5. Tari Schreider. Cybersecurity Law, Standards and Regulations: 2nd Edition. Rothstein Publishing, 2020. 326 p.
6. Модульне середовище для навчання MOODLE. Доступ до ресурсу: https://msn.khmnu.edu.ua/.
7. Електронна бібліотека університету. Доступ до ресурсу: http://library.khmnu.edu.ua/.

Викладач: кандидат технічних наук, доцент Чешун В.М.

ВСТУП

Дисципліна „Нормативно-правове забезпечення кібербезпеки” - складова професійної підготовки бакалаврів зі спеціальності „Кібербезпека”, є однією зі спеціальних профілюючих дисциплін.

Мета дисципліни. Формування системи знань міжнародних та національних стандартів, передових практик і політик інформаційної та кібербезпеки, розуміння предметної області щодо правил синтезу і реалізації політик безпеки як базису для дисциплін-кореквізитів і подальшої професійної діяльності із здатністю розв’язувати складні спеціалізовані задачі та практичні проблеми у галузі забезпечення інформаційної безпеки і\або кібербезпеки, що характеризуються комплексністю та неповною визначеністю умов.

Предмет дисципліни. Міжнародні та національні стандарти інформаційної та кібербезпеки, політики інформаційної та кібербезпеки.

Завдання дисципліни. Забезпечити набуття компетентностей та досягнення результатів навчання відповідно до Стандарту вищої освіти та освітньо-професійної програми підготовки бакалаврів зі спеціальності „Кібербезпека”:

компетентності:

КЗ 2. Знання та розуміння предметної області та розуміння професії.

КЗ 5. Здатність до пошуку, оброблення та аналізу інформації.

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.

результати навчання:

РН 3. Використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності.

РН 6. Критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності.

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 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).

Студент, який успішно завершив вивчення дисципліни, повинен: *застосовувати* набуті знання для розуміння предметної області та розуміння професії, *критично осмислювати* основні теорії, принципи, методи і поняття у навчанні та професійній діяльності; *приймати участь* у розробці, впровадженні та оцінці стратегії і політик інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації із застосуванням різних класів політик інформаційної безпеки та/або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів, сучасних принципах, способах та методах теорії захищених систем; *виконувати* пошук, оброблення, аналіз та синтез інформації з різних джерел інформації (державних та міжнародних стандартів тощо) для ефективного рішення спеціалізованих задач професійної діяльності; *застосовувати* державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі інформаційної та/або кібербезпеки на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів і для підготовки пропозицій до нормативних актів щодо забезпечення інформаційної та/або кібербезпеки; *застосовувати* здобуті знання міжнародних та національних стандартів, сучасних методів і моделей політик інформаційної безпеки та/або кібербезпеки, розуміння принципів і навички синтезу на їх основі політик безпеки для вирішення задач управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових); *застосовувати* знання державної та іноземних мов для вивчення міжнародних та національних стандартів, а також *використовувати* термінологію цих стандартів з метою забезпечення ефективності професійної комунікації.

СТРУКТУРА ЗАЛІКОВИХ КРЕДИТІВ ДИСЦИПЛІНИ

Назва теми	Кількість годин, відведених на:			
	лекції	практичні заняття	лабораторні роботи	самостійну роботу
Тема 1. Міжнародне регулювання інформаційної безпеки	16	16	-	38
Тема 2. Закони і стандарти Україні	18	18	-	44
Разом:	**34**	**34**	**-**	**82**

ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Зміст лекційного курсу

Номер лекції	Перелік тем лекцій, їх анотації	Кількість годин
Тема 1. Міжнародне регулювання інформаційної безпеки		
1	**Регулятивні складові інформаційної безпеки.** 1. Закони, стандарти, політики в інформаційній безпеці. 2. Правове забезпечення інформаційної безпеки в Україні (оглядове ознайомлення). Літ.: [3] с. 35-42, [4] с. 23-43	2
2	**Початок стандартизації, веселкова серія стандартів інформаційної безпеки.** 1. Початок стандартизації в інформаційній безпеці. 2. Введення до веселкової серії. 3. Помаранчева книга як фундамент веселкової серії 4. Критичний аналіз помаранчевої книги Літ.: [3] с.6-20; [2] с.13-31	2
3	**Розвиток веселкової серії стандартів інформаційної безпеки.** 1. Короткий огляд веселкової серії 2. Червона книга веселкової серії Літ.: [3] с. 21-28; [4] с.26-31	2
4	**Перші міжнародні стандарти Європи в галузі безпеки - ITSEC** 1. Історичні умови створення ITSEC. 2. Основні положення ITSEC 3. Роз'яснення основних положень ITSEC 4. Специфікації функцій безпеки стандарту ITSEC Літ.: [1] с.18-24; [2] с.22-27; [3] с.44-49	2
5	**Федеральні та Канадські критерії безпеки (стандарти FCITS і CTCPEC)** 1. Федеральні критерії безпеки інформаційних технологій FCITS 2. Канадські критерії безпеки комп'ютерних систем CTCPEC Літ.: [2] с.36-40	2
6	**Загальні критерії безпеки інформаційних технологій (стандарт ІСО/МЕК 15408)** 1. Загальні критерії безпеки інформаційних технологій 2. Угода про взаємне визнання сертифікатів Літ.: [1] с.25-33; [3] с.57-64	2
7	**Національні стандарти Германії (BSI) та Великобританії (BS 7799) в міжнародній стандартизації інформаційних технологій** 1. Стандарт Германії BSI 2. Стандарти Великобританії BS 7799 Літ.: [1] с.44-56	2
8	**Серії міжнародних стандартів інформаційної безпеки ISO/IEC 13335, 15408 та 27xxx (27k)** 1. Передумови появи серій міжнародних стандартів інформаційної безпеки 2. Серія ISO/IEC 13335 - Міжнародні стандарти безпеки інформаційних технологій 3. Серія ISO/IEC 15408 - Інформаційні технології: методи захисту - критерії оцінки. 4. Міжнародний стандарт ISO 27xxx – Міжнародні стандарти для системи управління інформаційною безпекою Літ.: [1] с.56-60; [2] с.76-81; [3] с.84-97	2

Тема 2. Закони і стандарти Україні		
9	**Стандартизація питань інформаційної безпеки в Україні** 1. Початок стандартизації інформаційної безпеки в Україні. 2. Дослідження практик введення в дію міжнародних стандартів ISO/IEC в якості ДСТУ Літ.: [1] с.70-84; [2] с.96-102; [3] с.108-120	2
10	**Закон України «Про основні засади забезпечення кібербезпеки України»** Літ.: [1] с.70-80	2
11	**Закон України Про захист інформації в інформаційнокомунікаційних системах** Літ.: [1] с.80-95	2
12	**Закон України Про інформацію** Літ.: [1] с.100-107	2
13	**Закон України Про науково-технічну інформацію** Літ.: [2] с.96-102	2
14	**Закон України Про державну таємницю** Літ.: [1] с.153-157	2
15	**Закон України «Про захист персональних даних»** Літ.: [1] с.110-117	2
16	**Об’єкти і суб’єкти інформаційної безпеки України** 1. Основні складові політики інформаційної безпеки держави 2. Визначення об'єктів та суб'єктів інформаційної небезпеки та їх обґрунтування. Літ.: [3] с. 35-42, [4] с. 23-43	2
17	**Концепція, стратегія та політика інформаційної безпеки підприємства** 1. Проблеми і засоби інформаційної безпеки – дві сторони політики 2. Ієрархічна модель інформаційної безпеки підприємства – концепція-стратегія-політика 3. Політика інформаційної безпеки: мета, задачі та основний зміст. Літ.: [1] с.85-93; [3] с.121-127	2
	Разом за семестр:	**34**

Зміст практичних занять

№ п/п	Теми практичних занять	Кількість годин
1	Синтез елементарної політики безпеки Літ.: [1] с.12-18; [4] с. 5-25; [9] с.12-58	4
2	Дослідження-настроювання політик безпеки операційних систем Літ.: [1] с.18-24; [4] с. 25-40	4
3	Дослідження політик безпеки провідних фірм IT-галузі Літ.: [1] с.25-26; [5] с. 58-70	4
4	Дослідження галузевих політик інформаційної безпеки установ і підприємств регіону Літ.: [2] с.25-26; [5] с. 58-70	4
5	Синтез базових видів політик безпеки: дискреційної, мандатної, рольової Літ.: [4] с. 1-72; [5] с. 50-87; [9] с. 115-180	4
6	Синтез і аудит політики безпеки в розрізі положень веселкової серії стандартів інформаційної безпеки Літ.: [3] с. 21-28; [4] с.26-31	4
7	Синтез і аудит політики безпеки на основі стандартів інформаційної безпеки ITSEC, FCITS і CTCPEC Літ.: [1] с.18-24; [2] с.22-40; [3] с.44-49	4
8	Синтез і аудит політики безпеки на основі стандартів ISO/IEC 13335, 15408 та 27xxx Літ.: [1] с.25-60; [2] с.76-81; [3] с.57-97	4
9	Підсумкове заняття**.** Дискусійне обговорення теорії та практик застосування політик і стандартів інформаційної безпеки. Тестування	2
	Разом за семестр:	**34**

Зміст самостійної (у т.ч. індивідуальної) роботи

На самостійне опрацювання студентів виноситься опрацювання лекційного матеріалу, підготовка до практичних занять. Керівництво самостійною роботою та виконанням реферативної роботи здійснює викладач згідно з розкладом консультацій в позаурочний час.

Номер тижня	Вид самостійної роботи	Кількість годин
1	Опрацювання теоретичного матеріалу, підготовка до ПЗ №1	4
2	Опрацювання теоретичного матеріалу, підготовка до презентації-захисту роботи за тематикою ПЗ №1	4
3	Опрацювання теоретичного матеріалу, підготовка до ПЗ №2	5
4	Опрацювання теоретичного матеріалу, підготовка до презентації-захисту роботи за тематикою ПЗ №2	5
5	Опрацювання теоретичного матеріалу, підготовка до ПЗ №3	5
6	Опрацювання теоретичного матеріалу, підготовка до презентації-захисту роботи за тематикою ПЗ №3	5
7	Опрацювання теоретичного матеріалу, підготовка до ПЗ №4	5
8	Опрацювання теоретичного матеріалу, підготовка до презентації-захисту роботи за тематикою ПЗ №4	5
9	Опрацювання теоретичного матеріалу, підготовка до ПЗ №5	5
10	Опрацювання теоретичного матеріалу, підготовка до презентації-захисту роботи за тематикою ПЗ №5	5
11	Опрацювання теоретичного матеріалу, підготовка до ПЗ №6	5
12	Опрацювання теоретичного матеріалу, підготовка до презентації-захисту роботи за тематикою ПЗ №6	5
13	Опрацювання теоретичного матеріалу, підготовка до ПЗ №4	5
14	Опрацювання теоретичного матеріалу, підготовка до презентації-захисту роботи за тематикою ПЗ №7	5
15	Опрацювання теоретичного матеріалу, підготовка до ПЗ №8	5
16	Опрацювання теоретичного матеріалу, підготовка до презентації-захисту роботи за тематикою ПЗ №8	5
17	Опрацювання теоретичного матеріалу, підготовка до дискусійного обговорення питань теорії та практик застосування політик і стандартів інформаційної безпеки, підготовка до ТК	4
	Разом за семестр:	**82**

Умовні позначення: ПЗ – практичне заняття, ТК – тестовий контроль

ТЕХНОЛОГІЇ ТА МЕТОДИ НАВЧАННЯ

Процес навчання з дисципліни ґрунтується на використанні традиційних та сучасних методів, зокрема: лекції (пояснювально-ілюстративні, репродуктивні); практичні/семінарські заняття (продуктивні, з використанням практикумів та тренінгових майстер-класів, аналітично-дослідницьких і творчих завдань для розвитку критичного мислення, продуктивних методів, з застосуванням інформаційно-комп'ютерних технологій).

Застосовувані при викладанні дисципліни методи навчання сприяють розвитку у студентів навичок soft skills: виконання частини практичних завдань проходить у формі рольових ігор і передбачає роботу у малих групах з призначенням тім-лідера, що сприяє розвитку лідерських якостей у студентів, здатності до спілкування і організації командної роботи над спільними задачами, а змінюваність умов задач і складу груп сприяє розвитку навичок адаптованості, гнучкості, комунікативності і оперативного налагоджування міжособистісних відносин в різних колективах; інтерактивне спілкування з проблемних питань під час лекцій, прилюдні виступи під час практичних занять і захисту реферативної роботи 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 і реферативної роботи, що орієнтовані на рішення проблемних завдань із застосуванням творчих підходів в аналізі і синтезі політик безпеки і орієнтацію на роботу з постійно оновлюваними міжнародними та національними стандартами; обмежений час на виконання практичних і тестових 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 визнання та зарахування результатів навчання здобувачів вищої освіти у ХНУ https://khmnu.edu.ua/wp-content/uploads/normatyvni-dokumenty/polozhennya/pro-poryadok-vyznannya-ta-perezarahuvannya-rezultativ-navchannya.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:

- усне опитування;
- практична перевірка (ділові ігри, презентації);
- тестування.

Семестровий контроль проводиться у формі заліку.

При виведенні підсумкової семестрової оцінки враховуються результати поточного контролю (залік за рейтингом формується автоматично за результатами поточного контролю).

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 - 5)	Тестовий контроль 1	Залік за рейтингом
Тема	1-2	1-2	
Ваговий коефіцієнт	0,75	0,25	

Оцінювання практичних занять. Оцінка, яка виставляється за практичне заняття, складається з таких елементів: здатність обрати вірний підхід у виконанні завдань і обґрунтувати зроблений вибір; правильність та самостійність виконання завдань (своєї складової загального завдання при застосуванні рольового розподілу відповідальності для ефективного рішення спеціалізованих задач професійної діяльності за предметом дисципліни), якість отримуваних результатів; вільне володіння студентом спеціальною термінологією і застосовуваними методами дисципліни, здатність критично осмислювати основні теорії, принципи, методи і поняття; уміння обґрунтувати прийняті рішення.

Оцінку, отриману на практичному занятті, викладач оголошує студенту одразу після його відповіді і проставляє в електронний журнал дисципліни.

Впродовж семестру студент має отримати на практичних заняттях щонайменше чотири позитивні оцінки, щоб виконати програму дисципліни.

Оцінювання тестових завдань. Тематичний тест для кожного студента складається з п’ятнадцяти тестових завдань, кожне з яких оцінюється одним балом. Максимальна сума балів, яку може набрати студент, складає 15.

Відповідність набраних балів за тестове завдання оцінці, що виставляється студенту

Сума балів за тестове завдання	1–5	6–10	11–13	14–15
Оцінка за 4-ри бальною шкалою	2	3	4	5

На тестування відводиться 15 хвилин (для закритої форми тестів – по одній хвилині на кожне завдання). Правильні відповіді студент записує у талоні відповідей. При цьому усі графи для відповідей мають бути заповнені цифрами, що відповідають правильним, на погляд студента, відповідям. Через 15 хвилин студенти здають викладачу завдання з талонами відповідей.

Тестування студент може також пройти і в он-лайн режимі в модульному середовищі для навчання MOODLE.

Оцінку за тестування викладач проставляє в електронний журнал дисципліни.

Оцінювання реферативної роботи. Оцінка, яка виставляється за реферативну роботу, складається з таких елементів: якість розкриття теми реферату; своєчасність захисту реферату; засвоєння студентом теоретичного матеріалу з дисципліни, вільне володіння студентом спеціальною термінологією дисципліни і уміння фахово обґрунтувати прийняті рішення та зроблені висновки; проявлені в роботі здатність виконувати пошук, оброблення, аналіз та синтез інформації з різних джерел інформації (державних та міжнародних стандартів тощо), а також здатність критично осмислювати основні теорії, принципи, методи і поняття дисципліни; якість оформлення реферативної складової роботи і презентації.

Оцінки за реферативну роботу викладач оголошує одразу після захисту і проставляє в

електронний журнал дисципліни.

Засвоєння студентом теоретичного матеріалу з дисципліни оцінюється за наведеними в таблиці критеріями оцінювання знань.

Критерії оцінювання знань студентів

Оцінка за інституційною шкалою	**Узагальнений критерій**
1	*2*
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.

Залік вважається зданим при отриманні студентом за зведеними результатами поточного контролю підсумкової оцінки з дисципліни від 3,00 до 5,00 балів. При цьому за вітчизняною шкалою ставиться оцінка за двобальною шкалою, а за шкалою ECTS – оцінка, що відповідає набраній студентом кількості балів.

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	Зараховано	***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	Незарахо-вано	***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. Види політик інформаційної безпеки.
2. Параметри політики безпеки.
3. Управління параметрами безпеки на основі політики.
4. Правила и взаємодія параметрів безпеки.
5. Адміністрування параметрів політики безпеки.
6. Політики диспетчера списку мереж.
7. Настройка параметрів політики безпеки.
8. Управління інформаційною безпекою та управління ризиками .
9. Ролі інформаційної безпеки.
10. Домени кібербезпеки.
11. Використання вимог по стандартизації до систем і процесів управління інформаційною безпекою.
12. Концепція та основні поняття зі стандарту COBIT.
13. Процесна модель COBIT.
14. Стандарти та специфікацій в області інформаційної безпеки.
15. Основні поняття і історія. Нормативна база. Канадські критерії оцінки безпеки надійних комп'ютерних систем.
16. Впровадження системи управління інформаційною безпекою згідно вимог міжнародніх стандартів.
17. Впроваджувати процесний підхід до створення СУІБ організації згідно вимог ISO IEC 27001 та 27002.
18. Організація системного захисту інформації на базі міжнародного стандарту ISO/IEC 27002 13.
19. Забезпечення безпеки інформаційних мереж та систем на базі міжнародного стандарту ISO/IEC 27002 15.
20. Організація захисту та створення безпечного зовнішнього середовища за стандартом ISO/IEC 17799 32.
21. Розробка політики інформаційної безпеки за стандартом ISO/IEC 17799 48.
22. Оцінка безпеки інформаційних технологій за стандартом ISO/IEC 15408 55.
23. Федеральні критерії оцінки безпеки надійних комп'ютерних систем.
24. Предмет інформаційної безпеки. Завдання інформаційної безпеки.
25. Тенденції та їх витоки трансформації процесів організації та проведення локальних та регіональних міждержавних конфліктів та війн.
26. Відображення цих процесів у національних та міжнародних нормативно-правових, доктринальних та стратегічних актах.
27. Основні функції системи забезпечення інформаційної безпеки України.
28. Основні елементи організаційної основи системи забезпечення інформаційної безпеки України.
29. Основні положення політики забезпечення інформаційної безпеки України.
30. Першочергові заходи щодо реалізації політики забезпечення інформаційної безпеки України.
31. Національні інтереси України в інформаційній сфері та шляхи їхнього забезпечення.
32. Загрози інформаційній безпеці України.
33. Джерела загроз інформаційній безпеці України.
34. Стан інформаційної безпеки України.
35. Завдання і забезпечення інформаційної безпеки України.
36. Класифікація загроз інформаційній безпеці.
37. Методики оцінки ризиків інформаційної безпеки.
38. Методи обробки ризиків інформаційної безпеки.

МЕТОДИЧНЕ ЗАБЕЗПЕЧЕННЯ

Навчальний процес з дисципліни „Нормативно-правове забезпечення кібербезпеки" повністю і в достатній кількості забезпечений необхідною навчально-методичною літературою, розміщеною в електронному варіанті в модульному середовищі.

РЕКОМЕНДОВАНА ЛІТЕРАТУРА

Основна

1. Микитишин А. Г. Комплексна безпека інформаційних мережевих систем: навчальний посібник / А.Г. Микитишин, М.М. Митник, П.Д. Стухляк. .– Тернопіль: ТНТУ, 2016. – 255 с.
2. Даник Ю.Г. Основи кібербезпеки та кібероборони: підручник / Ю. Г. Даник, П. П. Воробієнко, В. М. Чернега. – Видання друге, перероб. та доп. – Одеса : ОНАЗ ім. О.С. Попова, 2019. − 320 с.
3. Douglas J. Landoll Information Security Policies, Procedures, and Standards: A Practitioner's Reference / Douglas J. Landoll. – Boca Raton : CRC Press Taylor & Francis Group, 2016. – 246 p.
4. Practical Information Security: A Competency-Based Education Course / [Izzat Alsmadi, Robert Burdwell, Ahmed Aleroud, Abdallah Wahbeh, Mahmoud Ali Al-Qudah, Ahmad Al-Omari]. – Cham, Switzerland : Springer International Publishing AG, 2018. – 328 p.
5. Mair D. Information Security Standards / Dougal Mair, Shahn Harris (Lateral Security - IBM sub-contractor), Dougal Mair (ITS). – V1.4-draft. – Hillcrest : The University of Waikato, 2019. – 80 p.
6. Kim D. Fundamentals of information systems security / David Kim, Michael G. Solomon. – Third edition. – Burlington :Jones & Bartlett Learning, 2018. – 571 p.
7. Про національну безпеку України: Закон України [Електронний ресурс] / Затверджено Указом Президента України від 21 червня 2018 року № 2469^Ш – Режим доступу: https://zakon.rada.gov.ua/laws/show/2469-19. – Назва з екрану.
8. Стратегія кібербезпеки України [Електронний ресурс] / Указ Президента України від 15.01.2016 р. № 96/2016 – Режим доступу:. https://zakon5.rada.gov.Ua/laws/show/96/2016#n11. – Назва з екрану.
9. Стратегія національної безпеки України [Електронний ресурс] / Указ Президента України від 06.05.2015р. № 287/2015 – Режим доступу: https://zakon.rada.gov.ua/laws/show/287/2015**.** – Назва з екрану.
10. ДСТУ ISO/IEC 27032:2016 (ISO/IEC 27032:2012, IDT). Інформаційні технології. Методи захисту. Настанови щодо кібербезпеки. – Чинний від 2016-27-12. – Київ : ДП «УкрНДНЦ», 2018. – [50] с.

Додаткова

11. Common Criteria for Information Technology. Security Evaluation. Part 1: Introduction and general model. - April 2017. – Version 3.1, Revision 5. – 106 p.
12. Методи і алгоритми захисту інформаційних ресурсів комп'ютерних систем: навчальний посібник / В.М. Джулій, Ю.П. Кльоц, І.В. Муляр, В. М. Чешун. – Хмельницький: ХмНУ, 2020. – 196 с.
13. Nieles M. An Introduction to Information Security / Michael Nieles, Kelley Dempsey, Victoria Yan Pillitteri; Computer Security Division - Information Technology Laboratory. – NIST Special Publication 800-12, Revision 1. – Gaithersburg : National Institute of Standards and Technology, 2017. – 101 p.
14. Cybersecurity: Geopolitics, Law, and Policy / Amos N. Guiora; Professor of Law at the S.J. Quinney College of Law, University of Utah, USA. – New York : Taylor & Francis Books, 2017. – 177 p.
15. Information Security Standard: Information Technology Resource Management. – Virginia Information Technologies Agency (VITA), 2016. – 183 p.
16. Humphreys E. Implementing the ISO/IEC 27001:2013 ISMS Standard / Edward Humphreys. – Second Edition. – Norwood : Artech house, 2016. – 239 p.
17. Гладун А.Я. Таксономія стандартів інформаційної безпеки /А.Я. Гладун, К.О. Хала // Наука, технології, інновації. – 2017. – № 2. – С. 53-64
18. Shojaie B. Implementation of Information Security Management Systems based on the

ISO/IEC 27001 / Bahareh Shojaie. - Dissertation with the aim of achieving a doctoral degree at the Faculty of Mathematics, Informatics and Natural Sciences Department of Informatics of Universit¨at Hamburg. February 20, 2018. – 147 p.

19. Stephen Sakawa Kibwage. Role-Based Access Control Administration of Security Policies and Policy Conflict Resolution in Distributed Systems / Stephen Sakawa Kibwage. – A Dissertation submitted in partial fulfillment of the requirements for the degree of Doctor of Philosophy in Information Systems Graduate School of Computer and Information Sciences. – Nova Southeastern University, 2015. – 111 p.

20. Cyber-Development, Cyber-Democracy and Cyber-Defense: Challenges, Opportunities and Implications for Theory, Policy and Practice / Elias G. Carayannis, David F. J. Campbell, Marios Panagiotis Efthymiopoulos. – New York : Springer, 2014. – 360 p.

21. Кондратенко Ю. В. Візуальний аналіз політик безпеки в ERP-системах / Ю. В. Кондратенко, І. Г. Зотова, В. В. Грицюк // Збірник наукових праць Центру воєнно-стратегічних досліджень НУ оборони України ім. Івана Черняховського. – 2018. – № 1. – С. 68-73.

22. Stevens C. Assembling cybersecurity: The politics and materiality of technical malware reports and the case of Stuxnet / Clare Stevens // Contemporary Security Policy. – 2020. – Volume 41, Issue 1: Special issue: Cyber Security Politics. – P. 129-152.

23. Овсянніков В. В. Аналіз нормативно-правових та організаційно-технічних аспектів забезпечення інформаційної безпеки / [В. В. Овсянніков, С. В. Дехтяр, С. А. Паламарчук, Ю. О. Черниш, О. В. Шемендюк]. // Сучасні інформаційні технології у сфері безпеки та оборони. – 2015. – № 3(24). – С. 187-193.

24. Борсуковський Ю. В Визначення сучасних вимог щодо політики використання засобів криптографічного захисту інформації на підприємстві / Ю. В. Борсуковський // Сучасний захист інформації. – 2018. – № 1. – С. 74-81.

25. Ахрамович В. М. Адміністративний рівень інформаційної безпеки / В. М. Ахрамович // Сучасний захист інформації. – 2017. – № 1. – С. 10-14.

26. Дикий О. В. Стандарти інформаційної безпеки: компаративне дослідження / О. В. Дикий, М. О. Флюнт // Право та державне управлінняю – 2019. – № 2 (35), том 1. – С. 80-87.

27. Dunn M. Cyber security meets security politics: Complex technology, fragmented politics, and networked science / Myriam Dunn Cavelty, Andreas Wenger // Contemporary Security Policy. – 2020. – Volume 41, Issue 1: Special issue: Cyber Security Politics. – P. 5-32.

28. Hend K. Alkahtani. 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. – ISSN 1913-8989, E-ISSN 1913-8997. – Published by Canadian Center of Science and Education. – P. 117-125.

ІНФОРМАЦІЙНІ РЕСУРСИ

1. Інформаційне забезпечення у сфері технічного регулювання ДП "Укрметртестстандарт". Каталог НД України on-line. [Електронний ресурс]. – Режим доступу: http://csm.kiev.ua/index.php?option=com_content&view=article&id=3731&Itemid=154&lang=uk. – Назва з екрану.

2. Модульне середовище для навчання MOODLE. Доступ до ресурсу: https://msn.khmnu.edu.ua/.

3. Електронна бібліотека університету. Доступ до ресурсу: http://library.khmnu.edu.ua/.