СИЛАБУС КОМПОНЕНТИ ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ

”КОРПОРАТИВНА ТА ПРОФЕСІЙНА ЕТИКА В КІБЕРБЕЗПЕЦІ”

<table>
<tr><td colspan="3">Лектор курсу</td><td colspan="3">Туровський Олександр Леонідович,
доктор технічних наук, професор,
завідувач кафедри Технічних систем кіберзахисту</td><td>Контактна інформація лектора (e-mail),
сторінка курсу на платформі GWE</td><td>e-mail: o.turovskyi@duikt.edu.ua
сторінка курсу в GWE –
https://classroom.google.com/c/NzExNzA4Nzg5MTI3?cjc=kojz3fd
код курсу – kojz3fd</td></tr>
<tr><td colspan="3">Галузь знань</td><td colspan="3">12 Інформаційні технології</td><td>Рівень вищої освіти</td><td>магістр</td></tr>
<tr><td colspan="3">Спеціальність</td><td colspan="3">125 Кібербезпека та захист інформації</td><td>Семестр</td><td>1</td></tr>
<tr><td colspan="3">Освітньо-професійна програма</td><td colspan="3">Технічні системи інформаційного та кібернетичного захисту</td><td>Тип дисципліни</td><td>Основна компонента освітньо-професійної програми</td></tr>
<tr><td rowspan="2">Обсяг:</td><td>Кредитів ECTS</td><td>Годин</td><td colspan="5">За видами занять:</td></tr>
<tr><td>3</td><td>90</td><td>Лекцій: 12</td><td>Семінарських занять: -</td><td>Практичних занять: 18</td><td>Лабораторних занять: -</td><td>Самостійна підготовка: 60</td></tr>
<tr><td colspan="8">АНОТАЦІЯ КУРСУ</td></tr>
<tr><td colspan="3">Освітні компоненти для яких є базовою</td><td colspan="5">Організація проведення наукових досліджень, Ліцензування, атестація та сертифікація у сфері безпеки ОІД, Науково-педагогічна практика, Науково-дослідна практика</td></tr>
<tr><td>Мета курсу:</td><td colspan="7">формування у студентів базових теоретичних знань, необхідних для забезпечення цілісного уявлення щодо розуміння проблем професійної та корпоративної етики в технічних системах інформаційного та кібернетичного захисту, умінь застосовувати знання для аналізу, супроводу і контролю ефективної роботи колективу, вирішення проблем та впровадження заходів протидії кіберінцидентам</td></tr>
<tr><td colspan="8">Компетентності відповідно до освітньої програми</td></tr>
<tr><td colspan="4">Soft-skills / Загальні компетентності (КЗ)</td><td colspan="4">Hard-skills / Фахові компетентності (КФ)</td></tr>
</table>

КЗ-1. Здатність застосовувати знання у практичних ситуаціях. **КЗ-3.** Здатність до абстрактного мислення, аналізу та синтезу. **КЗ-4.** Здатність оцінювати та забезпечувати якість виконуваних робіт. **КЗ-5.** Здатність спілкуватися з представниками інших професійних груп різного рівня (з експертами з інших галузей знань / видів економічної діяльності).	**КФ 2.** Здатність розробляти, впроваджувати та аналізувати нормативні документи, положення, інструкції й вимоги технічного та організаційного спрямування, а також інтегрувати, аналізувати і використовувати кращі світові практики, стандарти у професійній діяльності в сфері інформаційної безпеки та/або кібербезпеки. **КФ 4**. Здатність аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації, формувати стратегію і політики інформаційної безпеки з урахуванням вітчизняних і міжнародних стандартів та вимог. **КФ 10**. Здатність провадити науково-педагогічну діяльність, планувати навчання, контролювати і супроводжувати роботу з персоналом, а також приймати ефективні рішення з питань інформаційної безпеки та/або кібербезпеки.

Програмні результати навчання (РН)

РН2. Інтегрувати фундаментальні та спеціальні знання для розв'язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах.
РН15. Зрозуміло і недвозначно доносити власні висновки з проблем інформаційної безпеки та/або кібербезпеки, а також знання та пояснення, що їх обґрунтовують, до персоналу, партнерів та інших осіб.
РН16. Приймати обґрунтовані рішення з організаційно-технічних питань інформаційної безпеки та/або кібербезпеки у складних і непередбачуваних умовах, у тому числі із застосуванням сучасних методів та засобів оптимізації, прогнозування та прийняття рішень.
РН17. Мати навички автономного і самостійного навчання у сфері інформаційної безпеки та/або кібербезпеки і дотичних галузей знань, аналізувати власні освітні потреби та об'єктивно оцінювати результати навчання.
РН18. Планувати навчання, а також супроводжувати та контролювати роботу з персоналом у напряму інформаційної безпеки та/або кібербезпеки.

ОРГАНІЗАЦІЯ НАВЧАННЯ

Тема, опис теми	Вид заняття	Оцінювання за тему	Форми і методи навчання/питання до самостійної роботи
МОДУЛЬ 1 "ОСНОВИ ПРОФЕСІЙНОЇ ТА КОРПОРАТИВНОЇ ЕТИКИ"			
Тема 1. Сучасна етика як практична філософія професійної діяльності у сфері кібербезпеки ***Знати:*** основні поняття та завдання професійної і корпоративної етики; етичні засади професійної та науково-педагогічної діяльності; принципові відмінності між етичними системами; засади формування й аргументованого	Лекція 1 2 год		Лекція-візуалізація. Пояснювально – ілюстративний вид викладу, експрес-опитування здобувачів
	Практичне заняття 1 2 год		Усне опитування, тематична навчальна дискусія. Аналіз етичних дилем професійної діяльності фахівця з кібербезпеки, обґрунтування та представлення професійної позиції.

представлення професійної позиції фахівця з кібербезпеки. ***Вміти:*** застосовувати етичний інструментарій для аналізу професійних ситуацій; формувати, обґрунтовувати та зрозуміло представляти власні висновки щодо етичних дилем; самостійно опрацьовувати професійні етичні стандарти та оцінювати власні освітні потреби. ***Формування компетенцій:*** КЗ-1, КЗ-3, КЗ-5, КФ 2, КФ 10 ***Результати навчання:*** РН2, РН15, РН17 ***Рекомендовані джерела:*** 1-5, 19, 25-26	Самостійна робота 8 год	5*	Самостійний аналіз міжнародних кодексів професійної етики у сфері ІТ та кібербезпеки; порівняння підходів і формування власного аргументованого висновку. Самооцінювання результатів навчання та визначення питань для подальшого опрацювання.

Тема 2. Професійна та корпоративна етика. Професіоналізм і відповідальність фахівця з кібербезпеки ***Знати:*** морально-нормативні засади професіоналізму, професійної відповідальності та корпоративної поведінки; механізми морально-нормативної регуляції професійної діяльності; принципи відповідального прийняття рішень у сфері кібербезпеки. ***Вміти:*** аналізувати професійні ситуації з позицій етичної відповідальності; аргументовано представляти професійну позицію; приймати обґрунтовані рішення в умовах конфлікту професійних, корпоративних та суспільних інтересів. ***Формування компетенцій:*** КЗ-1, КЗ-4, КЗ-5, КФ 4 ***Результати навчання:*** РН2, РН15, РН16 ***Рекомендовані джерела:*** 1-5, 19, 25-26	Лекція 2 2 год	5*	Лекція-візуалізація. Пояснювально – ілюстративний вид викладу, експрес-опитування здобувачів
	Практичне заняття 2 2 год		Усне опитування, тематична навчальна дискусія. Підготовка та представлення аргументованого професійного висновку щодо етично складної ситуації у сфері кібербезпеки; обґрунтування варіанта професійного рішення.
	Самостійна робота 8 год		Самостійний аналіз прикладів професійної відповідальності фахівців з кібербезпеки та корпоративних етичних стандартів. Підготовка короткого аналітичного висновку щодо наслідків етичних і неетичних управлінських рішень.
МОДУЛЬ 2 “ЕТИКА ПРОФЕСІЙНОЇ ДІЯЛЬНОСТІ В УПРАВЛІННІ ІНФОРМАЦІЙНОЮ ТА КІБЕРБЕЗПЕКОЮ”			
Тема 3. Інформаційна етика та етичні аспекти управління інформаційною безпекою ***Знати:*** принципи інформаційної етики; етичні вимоги до збору, обробки, використання та моніторингу інформації; співвідношення вимог безпеки, приватності та прав працівників; етичні аспекти управління інформаційною безпекою та	Лекція 3 2 год	5*	Лекція-візуалізація. Пояснювально – ілюстративний вид викладу, експрес-опитування здобувачів
	Практичне заняття 3 2 год		Усне опитування, тематична навчальна дискусія. Аналіз професійних ситуацій конфлікту між вимогами інформаційної безпеки, приватністю та правами працівників; обґрунтування етичного рішення під час реагування на інцидент.

реагування на інциденти. ***Вміти:*** аналізувати конфлікти між вимогами інформаційної безпеки, приватністю та правами людини; застосовувати етичні норми під час управління інформаційною безпекою і реагування на інциденти; самостійно оцінювати альтернативні підходи та обґрунтовувати етично прийнятні рішення. ***Формування компетенцій:*** КЗ-1, КЗ-4, КФ 4 ***Результати навчання:*** РН2, РН16, РН17 ***Рекомендовані джерела:*** 1-5, 9, 10, 13, 23, 25-26	Самостійна робота 8 год		Самостійне опрацювання етичних аспектів моніторингу, аудиту та реагування на інциденти інформаційної безпеки. Порівняння альтернативних підходів і самооцінювання сформованих навичок прийняття етичних рішень.
Тема 4. Професійна цифрова етика та етичні дилеми кібербезпеки	Лекція 4 2 год	5*	Лекція-візуалізація. Пояснювально – ілюстративний вид викладу, експрес-опитування здобувачів
Знати: основи професійної цифрової та комп'ютерної етики; етичні норми професійної комунікації у цифровому середовищі; типові моральні дилеми кібербезпеки, пов'язані з моніторингом, приватністю, розкриттям інформації та використанням цифрових технологій. ***Вміти:*** аналізувати моральні дилеми цифрової етики; формувати та аргументовано представляти професійне рішення з урахуванням інтересів працівника, організації та суспільства; самостійно оцінювати етичні наслідки цифрового моніторингу. ***Формування компетенцій:*** КЗ-1, КФ 2 ***Результати навчання:*** РН2, РН15, РН16, РН17 ***Рекомендовані джерела:*** 1-5, 8, 11, 12, 23, 24, 25-26	Практичне заняття 4 2 год		Усне опитування, тематична навчальна дискусія. Аналіз моральних дилем цифрової етики та аргументоване представлення професійного рішення з урахуванням інтересів працівника, організації та суспільства.
	Практичне заняття 5 2 год		Усне опитування, тематична навчальна дискусія. Аналіз етичних аспектів цифрового моніторингу працівників, використання соціальних мереж і захисту приватності в корпоративному середовищі.
	Самостійна робота 12 год		Самостійний аналіз сучасних кейсів цифрової етики у сфері кібербезпеки. Підготовка аргументованого висновку щодо меж допустимого моніторингу та самооцінювання власної готовності до вирішення етичних дилем.
Тема 5. Корпоративні кодекси, етична культура та робота з персоналом у сфері кібербезпеки	Лекція 5 2 год	5*	Лекція-візуалізація. Пояснювально – ілюстративний вид викладу, експрес-опитування здобувачів
Знати: принципи побудови професійних і корпоративних кодексів; роль етичної культури в системі кібербезпеки; механізми формування відповідальної поведінки персоналу; принципи етичного навчання, інструктажу, підвищення обізнаності та контролю дотримання норм персоналом. ***Вміти:*** розробляти положення корпоративного кодексу професійної поведінки; визначати етичні стандарти поведінки працівників; формувати програму етичного навчання та awareness-підготовки персоналу; доносити вимоги кодексу й	Практичне заняття 6 2 год		Усне опитування, тематична навчальна дискусія. Розроблення структури корпоративного кодексу професійної поведінки персоналу у сфері інформаційної та кібербезпеки; формулювання норм, відповідальності та механізмів їх комунікації.
	Практичне заняття 7 2 год		Усне опитування, тематична навчальна дискусія. Розроблення програми етичного навчання та підвищення обізнаності персоналу з питань інформаційної і кібербезпеки; визначення форм контролю засвоєння етичних вимог.

організовувати контроль їх виконання. ***Формування компетенцій:*** КЗ-1, КФ 2, КФ 4 ***Результати навчання:*** РН2, РН15, РН18 ***Рекомендовані джерела:*** 6, 7, 18, 20, 21, 25-26	Самостійна робота 12 год		Самостійний аналіз корпоративних кодексів і програм security awareness. Підготовка пропозицій щодо розвитку етичної культури та системи роботи з персоналом у підрозділі кібербезпеки.
Тема 6. Етика конфлікту, управління персоналом та прийняття етичних рішень у кібербезпеці ***Знати:*** види й причини професійних конфліктів у сфері кібербезпеки; етичні засади поведінки керівника і персоналу; принципи розподілу повноважень, відповідальності та професійної комунікації під час кіберінцидентів; методи прийняття етичних рішень. ***Вміти:*** вирішувати професійні конфлікти із застосуванням етичних норм; аргументовано комунікувати рішення; розподіляти ролі та відповідальність персоналу під час інциденту; застосовувати сценарний підхід і елементи теорії ігор для вибору обґрунтованого рішення. ***Формування компетенцій:*** КФ 10 ***Результати навчання:*** РН2, РН15, РН16, РН18 ***Рекомендовані джерела:*** 22, 14-17, 25-26	Лекція 6 2 год	5*	Лекція-візуалізація. Пояснювально – ілюстративний вид викладу, експрес-опитування здобувачів
	Практичне заняття 8 2 год		Усне опитування, тематична навчальна дискусія. Розв'язання конфліктних професійних ситуацій у сфері кібербезпеки; аргументація рішення та відпрацювання комунікації з персоналом.
	Практичне заняття 9 2 год		Метод сценаріїв, елементи теорії ігор. Моделювання кіберінциденту: організація комунікації, розподіл ролей і етичної відповідальності персоналу, прийняття колективного рішення та обговорення результатів.
	Самостійна робота 12 год		Самостійна підготовка сценарію професійного конфлікту або кіберінциденту з визначенням ролей персоналу, альтернативних рішень та етичних наслідків. Підготовка до екамену за дисципліну

МАТЕРІАЛЬНО-ТЕХНІЧНЕ ЗАБЕЗПЕЧЕННЯ ДИСЦИПЛІНИ

- програмні засоби підтримки прийняття рішень у сфері інформаційної безпеки («Вибір», Mpriority1.0)
- навчальна лабораторія Центр управління інформаційною та кібербезпекою (Security Operation Center)
- академічний центр компетенцій IBM «Кіберполігон»
- програмно-апаратні комплекси: IBM QRadar SIEM; IBM i2 Analyze Notebook Premium; Tenable Nessus Professional; ESET Protection.
- програмний комплекс для організації дистанційного навчання в мережі Internet MOODLE.

ІНФОРМАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ ДИСЦИПЛІНИ

1. Бралатан В. П., Гуцаленко Л. В., Здирко Н. Г. Професійна етика: Навч. посібник.- К.:Центр учбової літератури, 2011. – 252 с.
2. Легомінова С.В., Щавінський Ю.В., Мужанова Т.М., Якименко Ю.М., Капелюшна Т.В., Рабчун Д.І. Професійна етика управлінської діяльності в кібербезпеці. навч. посіб. Київ : ДУТ, 2023, 198 с.
3. О. Левицька. Професійна етика // Філософський енциклопедичний словник / В. І. Шинкарук (гол. редкол.) та ін. Київ : Інститут філософії імені Григорія Сковороди НАН України : Абрис, 2002. С. 531. 742 с. 1000 екз. ББК 87я2. ISBN 966-531-128-X.
4. Конотопець М. М., Сторчак А. С., Голь В. Д., **Туровський О. Л.** Вплив інформаційних технологій і світових практик на стандартизацію професій. Сучасний захист інформації. №1(61), 2025, С. 165-173. https://doi.org/: 10.31673/2409-7292.2025.015125
5. Weil, Vivian (2008 р.). Professional ethics (Професійна етика). URL:: http://ethics.iit.edu/teaching/professional-ethics.
6. Етика. Естетика.: навч.посібник. / за наук. ред.Панченко В. І. – К.: «Центр учбової літератури», 2014 – 432 с.
7. Професійна та корпоративна етика: навч. посіб. / за ред., В.І. Панченко. – К: 2019 ВПЦ «Київський університет», 2019 . 392 с..
8. Ломачинська І.М., Рихліцька О.Д., Барна Н.В. Основи корпоративної культури. Навч. посібник. К.: 2011., 480 с.
9. Уэбстер Ф. Теорії інформаційного суспільства. К., 2004. (перегkfl з англ)
10. Савченко В. А. Нейромережева технологія виявлення інсайдерських загроз на основі аналізу журналів активності користувачів / Савченко В. А., Савченко В. В., Довбешко С. В., Мацько О. Й., Зідан А. М. *Сучасний захист інформації* №4(36), 2018. С. 40-49.
11. Савченко В. А. Управління ризиками кібербезпеки на основі теоретико-ігрового підходу / Савченко В. А., Мацько О. Й. *Сучасний захист інформації* №2(38), 2019 . С. 6-16.
12. Методичні рекомендації щодо впровадження системи управління інформаційною безпекою та методики оцінки ризиків відповідно до стандартів Національного банку України. URL: https://zakon.rada.gov.ua/laws/show/v0365500-11 .
13. Савченко В. А. Модель інформаційного стримування між державами на основі теорії рефлексивних ігор / Савченко В. А., Дзюба Т. М. *Сучасний захист інформації* . №2(42), 2020. С. 6-18.
14. ДСТУ ISO/IEC 27035-1:2018.Інформаційні технології. Методи захисту. Керування інцидентами інформаційної безпеки. Частина 1. Принципи керування інцидентами(ISO/IEC 27035-1:2016, IDT).
15. ДСТУ ISO/IEC 27035-1:2018. Інформаційні технології. Методи захисту. Керування інцидентами інформаційної безпеки. Частина 2. Настанова щодо планування та підготовки до реагування на інциденти. (ISO/IEC 27035-1:2016, IDT).
16. ДСТУ ISO 19011:2019. Настанови щодо проведення аудитів систем управління. (ISO 19011:2018, IDT).
17. ДСТУ ISO 31000:2018.Менеджмент ризиків. (ISO 31000:2018, IDT).
18. Герчанівська П. Е. Культура управління : навч. посібник / Герчанівська П. Е. – К. : ІВЦ Видавництво “Політехніка”, 2005. 152 с.
19. Гах Й. М. Етика ділового спілкування : навч. посібник / Гах Й. М. – К. : Центр навч. літератури, 2005. – 160 с.
20. Ложкін Т. В. Психологія конфлікту: теорія і сучасна практика : навч. посібник / Т. В. Ложкін, Н.І. Пов’якель. К. : ВД «Професіонал», 2006. 416 с.
21. Морозова Т. Ю. Про необхідність вивчення комп’ютерної етики майбутніми ІТ-фахівцями / Т. Ю. Морозова URL: http://www.nbuv.gov.ua/portal/natural/vkpi/FPP/2006- 2/05Morozova.pdf .
22. Філіпова Л. Я. Комп'ютерна етика, інформаційна етика та кіберетика: сутність та співвідношення понять. Інформаційна діяльність: Проблеми науки, освіти та практики: матеріали міжнар. наук.-практ. конф. К, ДАККККМ, 2009. С.137-140.
23. Филиппова Л. Я., Зеленецкий В. С. Комп’ютерна етика. Морально-етичні і правові норми для користувачів комп’ютерних мереж: Навч. посібник. Харків: Вид-во «Кроссроуд», 2006. 209 с.
24. Якименко Ю. М. Про підхід до створення системи інформаційної безпеки в організації. Інформаційна безпека України: Зб. наук. доп. та тез НТК. Київ: Київський національний університет імені Тараса Шевченка(23-24 березня 2017року). С. 372-376.

25. Якименко Ю. М. Використання метрик для оцінки ефективності управління інцидентами інформаційної безпеки. Матеріали: інтернет-конференція "Актуальні проблеми інформаційної та кібернетичної безпеки" (26 жовтня 2018 року). Тези доповідей. Київ: ДУТ(ННІЗІ), 2018. С.69-71.
26. Інформаційні ресурси
Інформаційні технології у психології ч. 2. Електронний навчально-методичний комплекс /Щавінський Ю.В., Баранюк Н.І.// Львів: Національний університет «Львівська політехніка», 2018. № Е41-139-326/2020 від 12.10.2020 Тексти лекцій та практичних занять (електронний варіант).
27. Електронна бібліотека ДУІКТ.
Електронні матеріали в GWE: https://classroom.google.com/c/NzExNzA4Nzg5MTI3?cjc=kojz3fd
28. Інтернет-ресурси:
http://www.nbuv.gov.ua/ - сайт Національної бібліотеки України
http://www.scientific-library.net – Електронна бібліотека науково-технічної літератури
https://kneu.edu.ua/ua/science_kneu/ndi/prikl_etiki/ - сайт інституту прикладної та професійної етики

ПОЛІТИКА КУРСУ («ПРАВИЛА ГРИ»)

- Курс передбачає роботу в колективі.
- Середовище в аудиторії є дружнім, творчим, відкритим до конструктивної критики.
- Освоєння дисципліни передбачає обов'язкове відвідування лекцій і практичних занять, а також самостійну роботу.
- Самостійна робота включає в себе теоретичне вивчення питань, що стосуються тем лекційних занять, які не ввійшли в теоретичний курс, або ж були розглянуті коротко, їх поглиблена проробка за рекомендованою літературою.
- Усі завдання, передбачені програмою, мають бути виконані у встановлений термін.
- Якщо студент відсутній з поважної причини, він презентує виконані завдання під час самостійної підготовки та консультації викладача.
- Під час роботи над завданнями не допустимо порушення академічної доброчесності: при використанні Інтернет ресурсів та інших джерел інформації студент повинен вказати джерело, використане в ході виконання завдання. У разі виявлення факту плагіату студент отримує за завдання 0 балів.
- Студент, який спізнився, вважається таким, що пропустив заняття з неповажної причини з виставленням 0 балів за заняття, і при цьому має право бути присутнім на занятті.

За використання телефонів і комп'ютерних засобів без дозволу викладача, порушення дисципліни студент видаляється з заняття, за заняття отримує 0 балів.

*КРИТЕРІЇ ТА МЕТОДИ ОЦІНЮВАННЯ

Умовою допуску до підсумкового контролю є набрання студентом 30 балів у сукупності за всіма темами дисципліни

Форми контролю	Види навчальної роботи	Оцінювання
ПОТОЧНИЙ КОНТРОЛЬ	***Робота на заняттях за темами:***	
	Тема 1. Сучасна етика як практична філософія професійної діяльності у сфері кібербезпеки	5
	Тема 2. Професійна та корпоративна етика. Професіоналізм і відповідальність фахівця з кібербезпеки	5
	Тема 3. Інформаційна етика та етичні аспекти управління інформаційною безпекою	5
	Тема 4. Професійна цифрова етика та етичні дилеми кібербезпеки	5
	Тема 5. Корпоративні кодекси, етична культура та робота з персоналом у сфері кібербезпеки	5
	Тема 6. Етика конфлікту, управління персоналом та прийняття етичних рішень у кібербезпеці	5

	порядок оцінювання на заняттях : • участь у експрес-опитуванні за кожну правильну відповідь 0,25 бала • доповідь з презентацією за тематикою самостійного вивчення дисципліни (оцінка залежить від повноти розкриття теми, якості інформації, самостійності та креативності матеріалу, якості презентації і доповіді), підготовка реферату за кожну презентацію (реферат) максимум 3 бали • усне опитування, тестування, рішення практичних задач за кожну правильну відповідь 0,5 бала • участь у навчальній дискусії, обговоренні ситуаційного завдання за кожну правильну відповідь 2 бали • участь у діловій грі за кожну участь 1 бал ДОДАТКОВО за участь у наукових конференціях, підготовка наукових публікацій, участь у Всеукраїнських та Міжнародних конкурсах наукових робіт за спеціальністю, створення кейсів тощо. 5-10 балів	
	ВСЬОГО ЗА ПОТОЧНИЙ КОНТРОЛЬ	30
РУБІЖНЕ	Модульний контроль № 1 «ОСНОВИ ПРОФЕСІЙНОЇ ТА КОРПОРАТИВНОЇ ЕТИКИ»»	15 балів
ОЦІНЮВАННЯ (МОДУЛЬНИЙ КОНТРОЛЬ)	Модульний контроль № 2 «ЕТИКА ПРОФЕСІЙНОЇ ДІЯЛЬНОСТІ В УПРАВЛІННІ КІБЕРБЕЗПЕКОЮ»	15 балів
ПІДСУМКОВЕ ОЦІНЮВАННЯ ***Іспит***	Метою іспиту є контроль сформованості практичних навичок та професійних компетентностей, необхідних для виконання професійних обов'язків. Іспит проходить у письмовій або у тестовій формі	40 балів
	ВСЬОГО	100

ПІДСУМКОВА ОЦІНКА ЗА ДИСЦИПЛІНУ			
бали	**Критерії оцінювання**	**Рівень компетентності**	**Оцінка** */запис в екзаменаційній відомості*
90-100	Студент демонструє повні й міцні знання навчального матеріалу в обсязі, що відповідає робочій програмі дисципліни, правильно й обґрунтовано приймає необхідні рішенняв різних нестандартних ситуаціях. Вміє реалізувати теоретичні положення дисципліни в практичних розрахунках, аналізувати та співставляти дані об ‘єктів діяльності фахівця на основі набутих з даної та суміжних дисциплін знань та умінь. Знає сучасні технології та методи розрахунків з даної дисципліни. За час навчання при проведенні практичних занять, при виконанні індивідуальних / контрольних завдань проявив вміння самостійно вирішувати поставлені завдання, активно включатись в дискусії, може відстоювати власну позицію в питаннях та рішеннях, що розглядаються. Зменшення 100-бальної оцінки може бути пов’язане з недостатнім розкриттям питань, що стосується дисципліни, яка вивчається, але виходить за рамки об’єму матеріалу, передбаченого робочою програмою, або студент проявляє невпевненість в тлумаченні теоретичних положень чи складних практичних завдань.	**Високий** Повністю забезпечує вимоги до знань, умінь і навичок, що викладені в робочій програмі дисципліни. Власні пропозиції студента в оцінках і вирішенні практичних задач підвищує його вміння використовувати знання, які він отримав при вивчені інших дисциплін, а також знання, набуті при самостійному поглибленому вивчені питань, що відносяться до дисципліни, яка вивчається.	Відмінно / Зараховано (А)
82-89	Студент демонструє гарні знання, добре володіє матеріалом, що відповідає робочій програмі дисципліни, робить на їх основі аналіз можливих ситуацій та вміє застосовувати теоретичні положення при вирішенні практичних задач, але допускає окремі неточності. Вміє самостійно виправляти допущені помилки, кількість яких є незначною. Знає сучасні технології та методи розрахунків з даної дисципліни. За час навчання при проведенні практичних занять, при виконанні індивідуальних / контрольних завдань та поясненні прийнятих рішень, дає вичерпні пояснення.	**Достатній** Забезпечує студенту самостійне вирішення основних практичних задач в умовах, коли вихідні дані в них змінюються порівняно з прикладами, що розглянуті при вивчені дисципліни	Добре / Зараховано (В)

75-81	Студент в загальному добре володіє матеріалом, знає основні положення матеріалу, що відповідає робочій програмі дисципліни, робить на їх основі аналіз можливих ситуацій та вміє застосовувати при вирішенні типових практичних завдань, але допускає окремі неточності. Вміє пояснити основні положення виконаних завдань та дати правильні відповіді при зміні результату при заданій зміні вихідних параметрів. Помилки у відповідях/ рішеннях/ розрахунках не є системними. Знає характеристики основних положень, що мають визначальне значення при проведенні практичних занять, при виконанні індивідуальних / контрольних завдань та поясненні прийнятих рішень, в межах дисципліни, що вивчається.	**Достатній** Конкретний рівень, за вивченим матеріалом робочої програми дисципліни. Додаткові питання про можливість використання теоретичних положень для практичного використання викликають утруднення.	Добре / Зараховано (C)
64-74	Студент засвоїв основний теоретичний матеріал, передбачений робочою програмою дисципліни, та розуміє постанову стандартних практичних завдань, має пропозиції щодо напрямку їх вирішень. Розуміє основні положення, що є визначальними в курсі, може вирішувати подібні завдання тим, що розглядались з викладачем, але допускає значну кількість неточностей і грубих помилок, які може усувати за допомогою викладача.	**Середній** Забезпечує достатньо надійний рівень відтворення основних положень дисципліни	Задовільно / Зараховано (D)
60-63	Студент має певні знання, передбачені в робочій програмі дисципліни, володіє основними положеннями, що вивчаються на рівні, який визначається як мінімально допустимий. З використанням основних теоретичних положень, студент з труднощами пояснює правила вирішення практичних/розрахункових завдань дисципліни. Виконання практичних / індивідуальних / контрольних завдань значно формалізовано: є відповідність алгоритму, але відсутнє глибоке розуміння роботи та взаємозв'язків з іншими дисциплінами.	**Середній** Є мінімально допустимим у всіх складових навчальної програми з дисципліни	Задовільно / Зараховано (E)

35-59	Студент може відтворити окремі фрагменти з курсу. Незважаючи на те, що програму навчальної дисципліни студент виконав, працював він пасивно, його відповіді під час практичних робіт в більшості є невірними, необґрунтованими. Цілісність розуміння матеріалу з дисципліни у студента відсутні.	**Низький** Не забезпечує практичної реалізації задач, що формуються при вивчені дисципліни	Незадовільно з можливістю повторного складання) / Не зараховано(FX) *Взалікову книжку непроставляється*
1-34	Студент повністю не виконав вимог робочої програми навчальної дисципліни. Його знання на підсумкових етапах навчання є фрагментарними. Студент не допущений до здачі іспиту.	**Незадовільний** Студент не підготовлений до самостійного вирішення задач, які окреслює мета та завдання дисципліни	Незадовільно з обов'язковим повторним вивченням / Не допущений (F) *Взалікову книжку непроставляється*

ПОЛІТИКА ДОБРОЧЕСНОСТІ

Здобувач вищої освіти виконуючи самостійну або індивідуальну роботу повинен дотримуватись політики доброчесності.

У разі наявності плагіату в будь-яких видах робіт здобувача, він отримує незадовільну оцінку і повинен повторно виконати завдання, які передбачені у Силабусі.