# СИЛАБУС КОМПОНЕНТИ ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ

# «КОРПОРАТИВНА ТА ПРОФЕСІЙНА ЕТИКА В КІБЕРБЕЗПЕЦІ»

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| **Лектор курсу** | | | **Щавінський Юрій Віталійович,** кандидат технічних наук, доцент кафедри Управління інформаційною та кібернетичною безпекою . | | **Контактна інформація лектора (e-mail), сторінка курсу в Moodle** | **e-mail:** yushchavinsky@ukr.net; **сторінка курсу в Moodle –** Курс: Корпоративна та професійна етика в кібербезпеці (dut.edu.ua) | |
| **Галузь знань** | | | 12 Інформаційні технології | | **Рівень вищої освіти** | магістр | |
| **Спеціальність** | | | 125 Кібербезпека та захист інформації | | **Семестр** | 9 | |
| **Освітня програма** | | | Управління інформаційною та кібернетичною безпекою | | **Тип дисципліни** | Основна компонента освітньо-професійної програми | |
| **Обсяг:** | Кредитів ECTS | Годин | За видами занять: | | | | |
| | | | Лекцій | Семінарських занять | Практичних занять | Лабораторних занять | Самостійна підготовка |
| | 3 | 90 | 12 | - | 18 | - | 60 |

## АНОТАЦІЯ КУРСУ

| | |
|---|---|
| Освітні компоненти, які передують вивченню | |
| Освітні компоненти для яких є базовою | Педагогіка та психології у вищій школі, Організація проведення наукових досліджень,Управління інцидентами інформаційної безпеки, Управління проєктами інформаційної безпеки, Науково-педагогічна практика, Науково-дослідна практика |
| **Мета курсу:** | формування у студентів базових теоретичних знань, необхідних для забезпечення цілісного уявлення щодо розуміння проблем професійної та корпоративної етики в управлінні кібербезпекою, умінь застосовувати знання для аналізу, супроводу і контролю ефективної роботи колективу, вирішення проблем та впровадження заходів протидії кіберінцидентам |

**Компетентності відповідно до освітньої програми**

| **Загальні компетентності (КЗ)** | **Фахові компетентності (КФ)** |
|---|---|
| **КЗ-1.** Здатність застосовувати знання у практичних ситуаціях.<br>**КЗ-3.** Здатність до абстрактного мислення, аналізу та синтезу.<br>**КЗ-4.** Здатність оцінювати та забезпечувати якість виконуваних робіт.<br>**КЗ-5.** Здатність спілкуватися з представниками інших професійних груп різного рівня (з експертами з інших галузей знань / видів економічної діяльності).<br>**КЗ-7.** Здатність визначати підприємницькі можливості чи вид діяльності або громадського впливу, здатність приймати обґрунтовані рішення, здатність оцінювати та забезпечувати якість виконуваних робіт.<br>**КЗ-8**. Знання про стимули та бар'єри в ефективній командній роботі, вміння виявляти, | **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.<br>**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. |

| | |
|---|---|
| ставити та вирішувати проблеми.<br>**КЗ-9.** Володіння навичками критичного мислення. | **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)**

**РН1.** Вільно спілкуватись державною та іноземною мовами, усно і письмово для представлення і обговорення результатів досліджень та інновацій, забезпечення бізнес\операційних процесів та питань професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.
**РН7.** Обґрунтовувати використання, впроваджувати та аналізувати кращі світові стандарти, практики з метою розв'язання складних задач професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.
**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.
**РН18.** Планувати навчання, а також супроводжувати та контролювати роботу з персоналом у напряму інформаційної безпеки та/або кібербезпеки.
**РН27**. Здатність використовувати професійно профільовані знання й практичні навички для забезпечення результативної та ефективної взаємодії державних установ і організацій зі спеціальними та правоохоронними органами у сфері управління й забезпечення інформаційної безпеки.

## ОРГАНІЗАЦІЯ НАВЧАННЯ

| Тема, опис теми | Вид заняття | Оцінювання за тему | Форми і методи навчання/питання до самостійної роботи |
|---|---|---|---|
| **ЗМІСТОВИЙ МОДУЛЬ 1 «ОСНОВИ ПРОФЕСІЙНОЇ ТА КОРПОРАТИВНОЇ ЕТИКИ»** | | | |
| ***Тема 1. Сучасна етика як практична філософія кібербезпеки***<br>***Знати***: основні поняття предмету та завдань професійної та корпоративної етики; етичні засади науково-педагогічної діяльності; принципові відмінності між різними етичними системами та побудованими на них відповідними морально-нормативними вимогами та практиками.<br>***Вміти:*** володіти відповідним етичним інструментарієм для аналізу та прийняття рішень в конкретних ситуаціях професійної діяльності; застосовувати етичні норми при обґрунтовуванні використання, впровадженні та аналізі кращих світових стандартів, практик з метою розв'язання складних задач професійної діяльності в галузі управління інформаційною безпекою та кібербезпекою.<br>***Формування компетенцій:*** КЗ-1, КЗ-3, КЗ-5, КЗ-9, КФ 2, КФ 10<br>***Результати навчання:*** РН1, РН7, РН15<br>***Рекомендовані джерела:*** 1-5, 19, 25-26 | Лекція 1<br>2 год | 10* | Лекція-візуалізація |
| | Практичне заняття 1<br>2 год | | Практична робота, Аналітичний метод<br>Структура етичного знання: нормативна етика, професійна етика, корпоративна етика, етика наукової діяльності.<br>Взаємозв'язок і взаємовплив моралі і права. |
| | | | Практична робота, проблемно-пошуковий метод<br>Практичне використання етичних принципів у науково-педагогічній діяльності |

| | | | |
|---|---|---|---|
| ***Тема 2. Професійна та корпоративна етика в системі сучасного етичного знання. Професіоналізм як моральна цінність***<br>***<u>Знати</u>***: принципові відмінності між різними етичними системами та побудованими на них відповідними морально-нормативними вимогами та практиками; актуальні механізми та інструменти морально-нормативної регуляції професійної діяльності та корпоративного управління.<br>***<u>Вміти</u>***: застосовувати етичні норми при обґрунтовуванні використання, впровадженні та аналізі кращих світових стандартів, практик з метою розв'язання складних задач професійної діяльності в галузі управління інформаційною безпекою та кібербезпекою.<br>***<u>Формування компетенцій:</u>*** КЗ-4, КЗ-5, КФ 4<br>***<u>Результати навчання:</u>*** РН1, РН7<br>***<u>Рекомендовані джерела:</u>*** 1-5, 19, 25-26 | Лекція 2<br>2 год | 10* | Лекція-візуалізація |
| | Практичне заняття 2<br>2 год | | Дедуктивний метод, Практична робота<br>Професіоналізм як моральна риса особистості.<br><br>Аналітичний метод, Практична робота<br>Предмет та завдання корпоративної етики. |
| ***Тема 1. Сучасна етика як практична філософія кібербезпеки***<br><br>***Тема 2. Професійна та корпоративна етика в системі сучасного етичного знання. Професіоналізм як моральна цінність*** | Самостійна робота | | Аналітичний метод, Практична робота<br>1. Структура етичного знання.<br>2. Нормативна етика,<br>3. Професійна етика,<br>4. Корпоративна етика,<br>5. Етика наукової діяльності<br>6. Поняття і принципи науково-педагогічної етики.<br>7. Етичний сенс глобальних проблем сучасної цивілізації.<br>8. Глобальні проблеми сучасного світу та перспективи їх розв'язання.<br>9. Професійна етика як спосіб регуляції поведінки в конкретних видах професійної діяльності.<br>10. Роль професійної та корпоративної етики в становленні професіоналізму<br><br>Модульний контроль №1.<br>1. Виконання кваліфікаційних завдань. Тестування |
| **ЗМІСТОВИЙ МОДУЛЬ 2 «ЕТИКА ПРОФЕСІЙНОЇ ДІЯЛЬНОСТІ В УПРАВЛІННІ ІНФОРМАЦІЙНОЮ ТА КІБЕРБЕЗПЕКОЮ»** | | | |
| **Тема 3.** ***Інформаційна етика***<br>***<u>Знати</u>***: основи інформаційної етики, етичні норми концептуального підходу до побудови ефективної системи інформаційної безпеки.<br>***<u>Вміти</u>***: застосовувати знання етичних норм при створенні СУІБ | Лекція 3<br>2 год | 10* | Лекція-візуалізація, експрес-опитування |
| | Практичне | | Аналітичний метод, Практична робота<br>Інформаційна етика в контексті змін у сучасному суспільстві. |

| | | | |
|---|---|---|---|
| і системи управління інцидентами інформаційної безпеки (СУІБ) організації відповідно до вимог із стандартизації систем і процесів управління інформаційною безпекою, проводити аудит на відповідність СУІБ вимогам стандартів ISO, перевіряти СУІБ.<br>***Формування компетенцій:*** КЗ-9, КФ 4<br>***Результати навчання:*** РН7, РН15<br>***Рекомендовані джерела:*** 1-5, 9, 10, 13, 23, 25-26 | заняття 3<br>2 год | | Практична робота, проблемно-пошуковий метод<br>Розвиток інформаційної етики як сучасного напряму етичної думки і типу моральної регуляції сучасного суспільства. |
| ***Тема 3. Інформаційна етика*** | Самостійна робота | | Аналітичний метод, Практична робота<br>1. Інформаційна етика як моральна регуляція сучасного суспільства.<br>2. Інформаційне суспільство та інформаційна цивілізація. Інформаційна етика в просторі сучасних комунікативних процесів, в сучасній інформаційній та соціокультурній діяльності організацій.<br>3. Прикладна етика.<br>4. Аналіз інформаційної етики в контексті змін у сучасному суспільстві.<br>5. Розвиток інформаційної етики як сучасного напряму етичної думки і типу моральної регуляції сучасного суспільства |
| **Тема 4.** ***Професійна цифрова етика кібербезпеки***<br>***Знати***: основи професійної комп'ютерної етики, етичні норми спілкування в соціальних мережах.<br>***Вміти***: застосовувати знання комп'ютерної етики в професійній діяльності при управлінні інформаційною безпекою організацій.<br>***Формування компетенцій:*** КФ 2<br>***Результати навчання:*** РН7, РН16<br>***Рекомендовані джерела:*** 1-5, 8, 11,12, 23, 24, 25-26 | Лекція 4<br>2 год | 10* | Лекція-візуалізація, експрес-опитування |
| | Практичне заняття 4<br>2 год | | Практична робота, проблемно-пошуковий метод<br>Хакерська етика. Переваги і недоліки.<br>Обговорення результатів |
| | Практичне заняття 5<br>2 год | | Практична робота, проблемно-пошуковий метод<br>Методи та механізми розв'язання основних моральних дилем сучасних практик в сфері управління інформаційною та кібербезпекою. Обговорення результатів |
| ***Тема 4. Професійна цифрова етика кібербезпеки*** | Самостійна робота | | Практична робота<br>1. Поняття, принципи комп'ютерної етики.<br>2. Кодекс комп'ютерної етики.<br>3. Хакерська етика.<br>4. Філософія штучного інтелекту.<br>5. Етичні проблеми створення штучного розуму.<br>6. Комп'ютерна етика як професійна.<br>7. Етика інформаційної та кібербезпеки.<br>8. Методи та механізми розв'язання основних моральних дилем сучасних практик в сфері управління |

| | | | |
|---|---|---|---|
| | | | інформаційною та кібербезпекою |
| **Тема 5.** ***Корпоративні кодекси у сфері кібербезпеки***<br><br>***Знати***: актуальні механізми та інструменти морально-нормативної регуляції професійної діяльності та корпоративного управління, принципові відмінності між різними етичними системами та побудованими на них відповідними морально-нормативними вимогами та практиками.<br>***Вміти***: розробляти корпоративну методику управління інформаційною безпекою на основі кращих світових практик впровадження систем управління в сфері безпеки, застосовувати знання етичних норм при розробленні корпоративних кодексів організацій і підприємств.<br>***Формування компетенцій:*** КЗ-7, КФ 2, КФ 4<br>***Результати навчання:*** РН16, РН18, РН27<br>***Рекомендовані джерела:*** 6, 7, 18, 20, 21, 25-26 | Лекція 5<br>2 год | 10* | Лекція-візуалізація, експрес-опитування |
| | Практичне заняття 6<br>2 год | | Частково-пошуковий метод<br>Практична робота<br>Функції, які виконують корпоративні кодекси в організаціях.<br>Обговорення результатів |
| | Практичне заняття 7<br>2 год | | Практична робота, Частково-пошуковий метод<br>Професійні кодекси в сфері ІТ, інформаційній та кібернетичній безпеці. Обговорення результатів |
| ***Тема 5. Корпоративні кодекси у сфері кібербезпеки*** | Самостійна робота | | Практична робота<br>1. Поняття «кодексу корпоративної етики».<br>2. Типи корпоративних кодексів.<br>3. Основні функції, які виконують корпоративні кодекси в організаціях.<br>4. Характеристики відмінного кодексу.<br>5. Професійні кодекси в сфері ІТ, інформаційній та кібернетичній безпеці.<br>6. Особливості впровадження кодексів корпоративної етики у провідних компаніях світу та в Україні. |
| **Тема 6.** ***Етика конфлікту та методи прийняття етичних рішень в професійних ситуаціях управління кібербезпекою***<br>***Знати***: види, причини конфліктів в управлінні кібербезпекою, методи їх вирішення.<br>***Вміти***: вирішувати конфлікти із застосуванням етичних норм, застосовувати знання етичних норм при створенні СУІБ і системи управління інцидентами інформаційної безпеки (СУІІБ) організації відповідно до вимог із стандартизації систем і процесів управління інформаційною безпекою, проводити аудит на відповідність СУІБ вимогам стандартів ISO, перевіряти СУІБ, володіти відповідним етичним інструментарієм для аналізу та прийняття рішень в конкретних ситуаціях професійної діяльності. | Лекція 6<br>2 год | 10* | Лекція-візуалізація, експрес-опитування |
| | Практичне заняття 8<br>2 год | | Частково-пошуковий метод<br>Метод “мозкового штурму”<br>Конфлікти в управлінні кібербезпекою та методи їх визначення.<br>Обговорення результатів |
| | Практичне заняття 9<br>2 год | | Метод сценаріїв, Метод “теорії ігор”<br>Застосування етичних методів і засобів при управлінні інформаційними інцидентами і ризиками.<br>Обговорення результатів |

| | | | |
|---|---|---|---|
| ***Формування компетенцій:*** КЗ-8, КЗ-9, КФ 7, КФ 10<br>***Результати навчання:*** РН15, РН16, РН18, РН27<br>***Рекомендовані джерела:*** 22, 14-17, 25-26 | | | |
| ***Тема 6. Етика конфлікту та методи прийняття етичних рішень в професійних ситуаціях управління кібербезпекою*** | Самостійна робота | | Частково-пошуковий метод<br>Практична робота<br>1. Методи вивчення конфлікту.<br>2. Види та сутність конфліктів.<br>3. Методологічні засади конфліктології.<br>4. Методи подолання конфліктів.<br>5. Виокремлення наявних та потенційних моральних проблем в організації інформаційної безпеки корпорацій.<br>6. Етичні методи і засоби управління інформаційними інцидентами і ризиками, способи вирішення складних етичних ситуацій в управлінні інформаційною та кібербезпекою.<br>7. Використання відповідного етичного інструментарію для аналізу та прийняття рішень в конкретних ситуаціях професійної та ділової діяльності.<br>8. Етика конфлікту та методології прийняття етичних рішень в професійних ситуаціях.<br><br>Модульний контроль №2.<br>1. Виконання кваліфікаційних завдань. Тестування |

**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: навчальний посібник. Київ: 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: навчальний посібник. Київ : ДУТ, 2023, 198 с.
3. Легомінова С. В., Мужанова Т. М., Щавінський Ю. В., Якименко Ю. М., Запорожченко М. М., Рабчун Д. І. Аудит інформаційної безпеки : навчальний посібник. Київ : ДУТ, 2023. 125 с.
4. Якименко Ю. М., Легомінова С. В., Щавінський Ю. В., Рабчун Д. І. Управління інцидентами інформаційної безпеки. Сучасні методи і засоби : навчальний посібник. Київ : ДУТ, 2023. 243 с.
5. Мужанова Т.М., Щавінський Ю.В., Рабчун Д.І. Управління безпекою інформаційних мереж: навчальний посібник. Київ : ДУТ, 2023. с. 167.
6. О. Левицька, В. І. Шинкарук та ін. Професійна етика: філософський енциклопедичний словник. Київ: Інститут філософії імені Григорія Сковороди НАН України : Абрис, 2002. 531-742 с.
7. Davis, Michael. Language of professional ethics (Мова професійної етики). URL: http://ethics.iit.edu/teaching/language-professionalethics.
8. Weil, Vivian. Professional ethics (Професійна етика). URL: http://ethics.iit.edu/teaching/professional-ethics.

9. Панченко В. І. Етика. Естетика.: навчальний посібник. Київ: центр учбової літератури, 2014. 432 с.
10. Панченко В. І. Професійна та корпоративна етика: навчальний посібник. Київ: ВПЦ «Київський університет», 2019. 392 с.
11. Ломачинська І.М., Рихліцька О.Д., Барна Н.В. Основи корпоративної культури: навчальний посібник. Київ, 2011. 480 с.
12. Уэбстер Ф. Теорії інформаційного суспільства. Київ, 2004. (переклад з англ. мови)
13. Савченко В. А., Савченко В. В., Довбешко С. В., Мацько О. Й., Зідан А. М. Нейромережева технологія виявлення інсайдерських загроз на основі аналізу журналів активності користувачів /. Сучасний захист інформації №4(36). Київ, 2018, 40-49 с.
14. Савченко В. А., Мацько О. Й. Управління ризиками кібербезпеки на основі теоретико-ігрового підходу. Сучасний захист інформації №2(38). Київ,2019. 6-16 с.
15. 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 .
16. Савченко В. А. Дзюба Т. М. Модель інформаційного стримування між державами на основі теорії рефлексивних ігор. Сучасний захист інформації №2(42). Київ,2020. 6-18 с.
17. 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).
18. 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).
19. ДСТУ ISO 19011:2019. Настанови щодо проведення аудитів систем управління. (ISO 19011:2018, IDT).
20. ДСТУ ISO 31000:2018.Менеджмент ризиків. (ISO 31000:2018, IDT).
21. Герчанівська П. Е. Культура управління : навч. посібник. Київ: ІВЦ Видавництво "Політехніка", 2005. 152 с.
22. Гах Й. М. Етика ділового спілкування : навч. посібник. Київ: Центр навч. літератури, 2005. 160 с.
23. Ложкін Т. В., Пов'якель Н.І. Психологія конфлікту: теорія і сучасна практика : навч. посібник. Київ: ВД «Професіонал», 2006. 416 с.
24. Морозова Т. Ю. Про необхідність вивчення комп'ютерної етики майбутніми ІТ-фахівцями. URL: http://www.nbuv.gov.ua/portal/natural/vkpi/FPP/2006- 2/05Morozova.pdf .
25. 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. Київ: ДАКККМ, 2009. 137-140 с.
26. Філіпова Л. Я., Зеленецький В. С. Комп'ютерна етика. Морально-етичні і правові норми для користувачів комп'ютерних мереж: навч. посібник. Харків: вид-во «Кроссроуд», 2006. 209 с.
27. 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). 372-376 с.
28. Якименко Ю. М. *Використання метрик для оцінки ефективності управління інцидентами інформаційної безпеки*. Актуальні проблеми інформаційної та кібернетичної безпеки. матеріали міжнар. наук.-практ. конф. Київ: ДУТ(ННІЗІ), 2018. 69-71 с.
29. Щавінський Ю.В., Баранюк Н.І. Інформаційні технології у психології ч. 2. Електронний навчально-методичний комплекс. Львів : Національний університет «Львівська політехніка», 2018.
30. Тексти лекцій та практичних занять (електронний варіант).
31. Електронна бібліотека ДУІКТ.
32. Електронні матеріали в MOODLE : Курс: Корпоративна та професійна етика в кібербезпеці (dut.edu.ua)
33. Національна бібліотека України. URL: http://www.nbuv.gov.ua
34. Електронна бібліотека науково-технічної літератури. URL: http://www.scientific-library.net
35. Професійна етика. URL: https://www.unodc.org/documents/e4j/IntegrityEthics/E4J_Integrity_and_Ethics_Module_14_final_UKR.pdf
36. Інститут прикладної та професійної етики. URL: https://kneu.edu.ua/ua/science_kneu/ndi/prikl_etiki/

## 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,*** *у т.ч.:* | |
| | • присутність на заняттях (при пропусках занять з поважних причин допускається відпрацювання пройденого матеріалу) | за кожне відвідування 0,55 бала |
| | • 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 |
| **РУБІЖНЕ ОЦІНЮВАННЯ (МОДУЛЬНИЙ КОНТРОЛЬ)** | Модульний контроль № 1 «ОСНОВИ ПРОФЕСІЙНОЇ ТА КОРПОРАТИВНОЇ ЕТИКИ»» | максимальна оцінка – 15балів |
| | Модульний контроль № 2 «ЕТИКА ПРОФЕСІЙНОЇ ДІЯЛЬНОСТІ В УПРАВЛІННІ КІБЕРБЕЗПЕКОЮ» | максимальна оцінка –15 балів |
| **Додаткова оцінка** | Участь у наукових конференціях, підготовка наукових публікацій, участь у Всеукраїнських та Міжнародних конкурсах наукових робіт за спеціальністю, створення кейсів тощо. | Звільняється від іспиту |
| **ПІДСУМКОВЕ ОЦІНЮВАННЯ** ***Іспит*** | Метою іспиту є контроль сформованості практичних навичок та професійних компетентностей, необхідних для виконання професійних обов'язків.<br>Іспит проходить у письмовій формі. | 40 балів |

**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 рішення в різних нестандартних ситуаціях.<br>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.<br>Знає сучасні технології та методи розрахунків з даної | **Високий**<br>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 /<br>Зараховано (А) |

| | | | |
|---|---|---|---|
| | 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. | | |
| **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.<br>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**<br>Забезпечує студенту самостійне вирішення основних практичних задач в умовах, коли вихідні дані в них змінюються порівняно з прикладами, що розглянуті при вивчені дисципліни | Добре /<br>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**<br>Конкретний рівень, за вивченим матеріалом робочої програми дисципліни.<br>Додаткові питання про можливість використання теоретичних положень для практичного використання викликають утруднення. | Добре /<br>Зараховано (С) |
| **4 - 7** | Студент засвоїв основний теоретичний матеріал, | **Середній** | Задовільно / |

| | | | |
|---|---|---|---|
| | 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. . | Забезпечує достатньо надійний рівень відтворення основних положень дисципліни | 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**<br>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.<br>Цілісність розуміння матеріалу з дисципліни у студента відсутні. | **Низький**<br>Не забезпечує практичної реалізації задач, що формуються при вивчені дисципліни | Незадовільно з можливістю повторного складання) / Не зараховано (FX) *В залікову книжку не проставляється* |
| **1-34** | Студент повністю не виконав вимог робочої програми навчальної дисципліни.<br>Його знання на підсумкових етапах навчання є фрагментарними.<br>Студент не допущений до здачі іспиту. | **Незадовільний**<br>Студент не підготовлений до самостійного вирішення задач, які окреслює мета та завдання дисципліни | Незадовільно з обов'язковим повторним вивченням / Не допущений (F) *В залікову книжку не проставляється* |