



СИЛАБУС ДИСЦИПЛІНИ «Кіберетика»

Ступінь вищої освіти - Магістр
 Спеціальність 011 Освітні, педагогічні науки
 Освітня програма «Інформаційно-комунікаційні технології в освіті»

Рік навчання 1 семестр 1-2

Форма навчання денна, заочна (денна, заочна)

Кількість кредитів ЄКТС 4

Мова викладання українська (українська, англійська, німецька)

Лектор курсу
 Контактна інформація
 лектора (e-mail)
 Сторінка курсу в eLearn

Єресько Олег Вікторович

ieresko.o@ukr.net

ОПИС ДИСЦИПЛІНИ

(до 1000 друкованих знаків)

Курс розглядає морально-етичні норми комп'ютерної етики, основи професійної та прикладної етики, етики Інтернету; професійні етичні норми та правила для «комп'ютерних професіоналів», типи їх взаємовідносин; правове регулювання етики комп'ютерних співвідношень; інформаційні злочини, злочини в мережі Інтернет, кібербулінг, відповідальність за них, засоби їх попередження та запобігання; етико-правові проблеми охорони інтелектуальної власності та авторського права в мережі Інтернет.

СТРУКТУРА КУРСУ

Тема	Години (лекції/практичні)	Результати навчання	Завдання	Оцінювання
1, 2 семестри				
Модуль I. МОРАЛЬНО-ЕТИЧНІ НОРМИ КІБЕРЕТИКИ				
Тема 1. Основи професійної етики	2/2	<p><i>Знати основні поняття:</i> професійні моральні норми, етика, професійна етика, педагогічна етика, кіберетика (інформаційна, комп'ютерна етика), професійний етичний кодекс</p> <p><i>Вміти:</i> характеризувати напрями розвитку професійної етики: відносини трудових колективів і кожного фахівця окремо; моральні якості особистості фахівця; взаємини в професійних колективах та специфічні моральні норми, властиві для освітянського середовища; особливості професійного виховання;</p> <p><i>Аналізувати:</i> основні види професійної етики та специфічних вимог в області моралі (педагогічна етика, комп'ютерна етика тощо);</p> <p><i>Розуміти:</i> взаємозв'язок та співвідносини теоретичної, прикладної (практичної) та професійної етики;</p> <p><i>Застосовувати:</i> отриманні знання та навички у практичній діяльності</p>	<i>Підготовка та виступи на практичних заняттях</i>	5

<p>Тема 2. Кіберетика: вступ у проблематику</p>	<p>2/2</p>	<p><i>Знати основні поняття:</i> кіберетика (етика Інтернет, віртуальна етика, комп'ютерна етика, мережевий етикет, нетикет, webethics, кодекси кіберетики, моральні норми в комп'ютерному середовищі, національні кодекси кіберетики <i>Вміти:</i> доводити значення моральних норм в комп'ютерному середовищі як історично сформовану основу для розробки нових та вдосконалення існуючих юридичних норм, що забезпечуються силою державного впливу; <i>Аналізувати:</i> значення кодексів етики асоціацій розробників інформаційних технологій, менеджерів інформаційних технологій, користувачів інформаційних технологій, сертифікованих комп'ютерних професіоналів <i>Розуміти:</i> комп'ютерну етику як складне динамічне поле досліджень, що передбачає аналіз відносин між фактами, концепціями, політикою і цінностями в контексті інтенсивного розвитку інформаційно-комп'ютерних технологій <i>Застосовувати:</i> отриманні знання та навички у практичній діяльності</p>	<p><i>Підготовка та виступи на практичних заняттях</i></p>	<p>5</p>
<p>Тема 3. Інформаційна етика. Етика Інтернету</p>	<p>4/4</p>	<p><i>Знати основні поняття:</i> інформаційна етика, етика Інтернету, нетикет, кіберпростір <i>Вміти:</i> ілюструвати особливості етичних норм для користувачів мережі Інтернет, правила «нетикету»; <i>Аналізувати:</i> проблеми протиріччя між позитивним впливом нових можливостей користування інформацією з мережі та негативними наслідками; <i>Розуміти:</i> значення положень освітньої політики в сфері інформатизації суспільства, яка має поєднувати багатий потенціал інформаційних і телекомунікаційних технологій та збереження культурної спадщини (національні традиції, культурні цінності та норми) кожного народу світового співтовариства. <i>Застосовувати:</i> отриманні знання та навички у практичній діяльності</p>	<p><i>Підготовка та виступи на практичних заняттях</i></p>	<p>10</p>
<p>Тема 4. Професійні етичні норми та правила для «комп'ютерних»</p>	<p>5/4</p>	<p><i>Знати основні поняття:</i> комп'ютерні професіонали, стандарти поведінки, лояльність, моральні основи взаємовідносин; <i>Вміти:</i> характеризувати типи взаємовідносин комп'ютерних професіоналів з такими категоріями, як: роботодавці; клієнти; колеги по професії; громадськість.</p>	<p><i>Підготовка та виступи на практичних заняттях, задача проміжного</i></p>	<p>15</p>

професіоналів»		<p><i>Аналізувати:</i> співвідношення між професійними знаннями та відповідальністю;</p> <p><i>Розуміти:</i> поняття «комп'ютерних професіоналів»: програмісти, системні аналітики, системотехніки, оператори, інформаційні працівники (посередники), продавці комп'ютерного устаткування, користувачі продуктів інформаційнокомп'ютерних технологій;</p> <p><i>Застосовувати:</i> отриманні знання та навички у практичній діяльності</p>	модульного оцінювання	
----------------	--	--	-----------------------	--

Модуль II. ПРАВОВІ НОРМИ КІБЕРЕТИКИ

<p>Тема 5. Інформаційно-правові основи регулювання комп'ютерних співвідносин. Інформаційні злочини</p>	4/4	<p><i>Знати основні поняття:</i> інформаційні злочини (кіберзлочини), основні групи кіберзлочинів, кібербулінг, його різновиди: хепіслепінг; тролінг; флеймінг; онлайн-грумінг; секстинг;</p> <p><i>Вміти:</i> характеризувати інформаційні правовідносини як такі, що виникають за умов: формування та використання інформаційних ресурсів на основі створення, збору, обробки, збереження, пошуку, розповсюдження та надання користувачеві інформації і документів; створення та використання інформаційних технологій та засобів їх забезпечення; захисту інформації та прав суб'єктів, що беруть участь в інформаційних процесах;</p> <p><i>Аналізувати:</i> основні групи інформаційних злочинів за родовим об'єктом: проти особистості, її здоров'я; в сфері економіки; проти суспільної безпеки і суспільного порядку; проти державної влади; проти миру та безпеки людства;</p> <p><i>Розуміти:</i> небезпеку кібербулінгу як одного із різновидів булінгу (цькування) - форми агресії, що передбачає жорстокі дії з метою дошкулити, нашкодити, принизити людину з використанням інформаційно-комунікаційних засобів: мобільних телефонів, електронної пошти, соціальних мереж тощо;</p> <p><i>Застосовувати:</i> отриманні знання та навички у практичній діяльності</p>	<p><i>Підготовка та виступи на практичних заняттях, захист реферативного дослідження</i></p>	15
<p>Тема 6. Комп'ютерні злочини в мережі Інтернет: правова оцінка, засоби їх попередже</p>	2/2	<p><i>Знати основні поняття:</i> комп'ютерні злочини, інформаційні війни, кібербезпека, комп'ютерна інформація, комп'ютерний вірус;</p> <p><i>Вміти:</i> давати визначення комп'ютерних злочинів як передбачених кримінальним законом суспільно небезпечних дій, у яких комп'ютерна інформація є об'єктом злочинного зазіхання;</p>	<p><i>Підготовка та виступи на практичних заняттях</i></p>	5

ння та запобігання		<i>Аналізувати:</i> основні категорії комп'ютерних злочинів: 1) злочини, зв'язані з втручанням у роботу комп'ютерів і 2) злочини, що використовують комп'ютери як необхідні технічні засоби; <i>Розуміти:</i> основні групи мір попередження комп'ютерних злочинів: правові, організаційно-технічні та криміналістичні; <i>Застосовувати:</i> отриманні знання та навички у практичній діяльності		
Тема 7. Етико-правові проблеми охорони інтелектуальної власності та авторського права в мережі Інтернет	4/4	<i>Знати основні поняття:</i> інтелектуальна власність, авторське право, академічна доброчесність, плагіат, інформаційне право; <i>Вміти:</i> доводити необхідність захисту авторських прав в мережі Інтернет; <i>Аналізувати:</i> основні типи об'єктів інтелектуальної власності в мережі: промислові, комерційні і художні роботи, комп'ютерні програми, торговельні марки тощо; <i>Розуміти:</i> специфіку етико-правових проблем авторського права в дистанційній освіті: політика захисту авторського права та інтелектуальної власності; програмне забезпечення курсів та проблеми їх ліцензування; загальні проблеми авторського права; <i>Застосовувати:</i> отриманні знання та навички у практичній діяльності	<i>Підготовка та виступи на практичних заняттях, задача проміжного модульного оцінювання</i>	15
Всього за 1-2 семестри				70
Екзамен				30
Всього за курс				100

ПОЛІТИКА ОЦІНЮВАННЯ

<i>Політика щодо дедлайнів та перескладання:</i>	Роботи, які здаються із порушенням термінів без поважних причин, оцінюються на нижчу оцінку. Перескладання модулів відбувається із дозволу лектора за наявності поважних причин (наприклад, лікарняний).
<i>Політика щодо академічної доброчесності:</i>	Списування під час модульної роботи та екзамену заборонені (у т.ч. із використанням мобільних девайсів). Реферати повинні мати коректні текстові посилання на використану літературу
<i>Політика щодо відвідування:</i>	Відвідування занять є обов'язковим і також забезпечує додаткові бали. За об'єктивних причин (наприклад, хвороба, міжнародне стажування) навчання може відбуватись індивідуально (в он-лайн формі за погодженням із деканом факультету)

ШКАЛА ОЦІНЮВАННЯ СТУДЕНТІВ

Рейтинг здобувача вищої освіти, бали	Оцінка національна за результати складання екзаменів заліків	
	екзаменів	заліків
90-100	відмінно	зараховано
74-89	добре	
60-73	задовільно	
0-59	незадовільно	не зараховано