СИЛАБУС КУРСУ
«ПРОТИДІЯ КІБЕРЗЛОЧИННОСТІ»

Ступінь вищої освіти - бакалавр
Освітньо-професійна програма: **Право**
Галузь знань: **08 Право**
Спеціальність: **081 Право**
Компонент освітньої програми – вибіркова дисципліна
Рік підготовки – 4 рік, семестр - 8
Кількість кредитів: 4
Мова викладання: українська
Дні занять: згідно з розкладом
Консультації: згідно з розкладом

Керівник курсу – **Івасьєв Степан Володимирович**, викладач ЦК комп'ютерних дисциплін, кандидат технічних наук, доцент
Контактна інформація - *stepan.ivasiev@gmail.com*

АНОТАЦІЯ ДИСЦИПЛІНИ

Дисципліна ***«Протидія кіберзлочинності»*** спрямована на формування у здобувачів освіти компетентностей для визначення місця і ролі кібербезпеки в загальній системі національної безпеки, стану та принципів забезпечення інформаційної безпеки особистості, суспільства та держави, необхідних для подальшої роботи та навчити їх застосуванню методів та засобів ефективного та безпекового поводження з інформацією незалежно від її походження та виду в умовах широкого використання сучасних інформаційних технологій.

Предметом вивчення є міжнародне та Українське законодавство у сфері кібербезпеки та інформаційної безпеки та розгляд загальних підходів до кіберінцидентів.

Навчальна дисципліна спрямована на формування у студентів професійних навичок у сфері протидії кіберзлочинності та захисту інформації, а саме нормативно - правових засад та технічних аспектів.

СТРУКТУРА КУРСУ ТА ЗАВДАННЯ ВИВЧЕННЯ ДИСЦИПЛІНИ

Кількість годин (аудит./ самост.)	**Тема**	**Результати навчання**	**Форми контролю**
22/40	**Змістовий модуль І. Нормативно-правові акти України**		
4/8 Л1, С1	**Тема 1.** Учасники кіберпростору, кібербезпека, загальні питання управління безпекою.	Знати основні терміни кібербезпеки. Знати взаємозв'язки у кіберпросторі. Знати схеми взаємодії учасників кіберпростору. Знати концепції ведення кіберборотьби та фактори впливу на кібербезпеку. Вміти проводити класифікацію учасників кіберпростору.	Питання, презентаційні проекти, тести

Кількість годин (аудит./ самост.)	Тема	Результати навчання	Форми контролю
4/8 Л2, С2	**Тема 2.** Нормативно-правові акти, які закріплюють концептуальні положення кібербезпеки в Україні	Знати ієрархію нормативних актів, Конституції України та закону України «Про національну безпеку». Знати визначення термінів та стратегію національної безпеки України. Знати основні пункти законів України «Про інформацію», «Про доступ до публічної інформації», «Про захист персональних даних», «Про державну таємницю», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про радіочастотний ресурс», «Про телекомунікації», «Про захист суспільної моралі», «Про оборону України», «Про Збройні Сили України», «Про Службу безпеки України», «Про Державну службу спеціального зв'язку та захисту інформації». Вміти виявити ознаки порушення законів України в сфері кібербезпеки, захисту і опрацювання інформації.Вміти надавати загальну характеристику кіберзлочинів.	Питання, тестові завдання
4/8 Л3, С3	**Тема 3.** Нормативно-правові акти, які закріплюють визначальні положення щодо забезпечення кібербезпеки в Україні	Знати основні положення Указу Президента «Про Стратегію кібербезпеки України» та Закон України «Про Основні засади розвитку інформаційного суспільства в Україні». Знати основні принципи стратегії розвитку інформаційного суспільства в Україні, Закон України «Про Національну програму інформатизації», Закон України «Про Концепцію Національної програми інформатизації», Концепція формування системи національних електронних інформаційних ресурсів. Положення про Національний реєстр електронних інформаційних ресурсів. Вміти застосовувати Закон України «Про захист персональних даних».	Захист міні-проектів, питання
4/8 Л4, С4	**Тема 4.** Нормативно-правові акти, які визначають порядок охорони державної таємниці в Україні	Знати закон України «Про державну таємницю» та визначення термінів. Знати законодавство України про державну таємницю. Знати основні принципи державної політики щодо державної таємниці. Вміти розділяти компетенцію державних органів, органів місцевого самоврядування та їх посадових осіб у сфері охорони державної таємниці. Вміти застосовувати те реалізовувати права на секретну інформацію та її матеріальні носії. Вміти виділяти інформацію, що може бути віднесена до державної таємниці.	Захист міні-проектів, **модульний контроль**
6/8 Л5, Л6, С5	**Тема 5.** Закони України про електронний документообіг та електронний цифровий підпис	Знати визначення основних термінів та законодавство про електронні документи та електронний документообіг. Знати основні принципи державного регулювання електронного документообігу. Знати правовий статус електронного документа та його копії. Вміти виконувати перевірку цілісності та автентичності цифрового підпису електронного документа. Вміння використовувати електронний документ та електронний підпис.	

Кількість годин (аудит./ самост.)	Тема	Результати навчання	Форми контролю
20/38	**Змістовий модуль 2. Забезпечення технічного захисту інформації**		
4/8 Л7, С6	**Тема 6.** Кіберзлочинність: поняття, види та запобігання.	Знати поняття кіберзлочинності та її місце в загальній структурі злочинності. Знати основні принципи європейського конвенційного механізму запобігання кіберзлочинності: поняття та система. Знати детермінанти та основні напрямки запобігання кіберзлочинності.	Питання, тестові завдання
4/6 Л8, С7	**Тема 7.** Кримінально-правове забезпечення боротьби з кіберзлочинністю.	Знати сучасний стан кримінально-правового забезпечення боротьби з кіберзлочинністю. Знати реалізацію форм кримінальної відповідальності за кіберзлочини. Вміти надавати загальну характеристику кіберзлочинів.	Питання, практичні завдання/задачі
4/6 Л9, С8	**Тема 8.** Кібербезпека – загрози, вразливості та атаки.	Знати шкідливе програмне забезпечення та зловмисний код. Знати основні принципи функціонування: Вірусів, Інтернет-черв'яків та «Троянських коней», Логічні бомби (Logic Bombs), програми – вимагачі. Вміти виділяти типи шкідливого ПЗ.	Питання, практичні завдання/задачі
4/10 Л10, С9	**Тема 9**. Соціальна інженерія.	Знати основні принципи соціальної інженерії та тактики соціальної інженерії. Знати методи обману. "Серфінг через плече" і “Дайвінг у смітнику”. Знати основні підходи «Уособлення і розіграшу» та способи несанкціонованого проникнення. Знати способи шахрайства в Інтернеті та по електронній пошті.	Захист міні-проектів, питання
4/8 Л11, С10	**Тема 10.** Державні стандарти України в сфері забезпечення технічного захисту інформації	Знати принципи застосування ДСТУ 3396.0-96 «Захист інформації Технічний захист інформації. Основні положення», ДСТУ 3396.1-96 «Захист інформації Технічний захист інформації. Порядок проведення робіт» та ДСТУ 3396.2-97 «Захист інформації Технічний захист інформації. Терміни та визначення».	Реферати-повідомлення, **модульний контроль**

СХЕМА ВИВЧЕННЯ ДИСЦИПЛІНИ

Семестр VIII

	1 тиждень	2 тиждень	3 тиждень	4 тиждень	5 тиждень	6 тиждень	7 тиждень	8 тиждень	9 тиждень	10 тиждень	11 тиждень	12 тиждень	13 тиждень	14 тиждень	15 тиждень	16 тиждень	17 тиждень
Лекції	Л1	Л2	Л3		Л4	Л5	Л6	Л7	Л8		Л9	Л 10	Л11 1				
Семінарські заняття	С1		С2	С3	С4		С5		С6	С7	С8		С 9	С1 0			
Контроль знань							МК 1						МК 2	ІН ДЗ			

Л1 - лекції
С1 - семінарське заняття по темі 1
МК1 - модульний контроль 1
ІНДЗ - індивідуальне навчально-дослідне завдання

ПОЛІТИКА ПРОВЕДЕННЯ АУДИТОРНИХ ЗАНЯТЬ

Для якісного засвоєння курсу необхідна систематична та усвідомлена робота студентів в усіх видах навчальної діяльності: лекції, семінарські заняття, консультації, самостійна робота як індивідуальна, так і під керівництвом викладача.

При проведенні аудиторних занять домінуючими є проблемні, індивідуально-диференційовані, особистісно-орієнтовані форми проведення занять та технології компетентнісного навчання.

На лекціях у формі активної бесіди з елементами навчальної дискусії розглядаються основні теоретичні положення теми, які вимагають роз'яснення та уточнення з боку викладача. На лекціях вимагається активна участь студентів у обговоренні ключових положень теми, ведення стислого конспекту лекції.

Теоретичні знання, отримані студентами під час лекцій, обговорюються більш детально на **семінарських заняттях** у формі міні-дискусій, представлення міні-проектів, розв'язування практичних завдань (кейсів), розгляду правових ситуацій, складання правових і процесуальних документів.

При підготовці до семінарських занять студент опрацьовує теоретичні питання відповідно до плану заняття, звертаючи увагу на вимоги щодо оформлення (складання таблиць, структурно-логічних схем, глосаріїв, конспектів тощо). Інформаційними джерелами для здобувачів освіти є конспект лекцій та наведений у навчальних матеріалах перелік рекомендованої літератури щодо кожної теми. За наявності серед завдань семінарського заняття підготовки реферату – робота здобувачів освіти полягає у підготовці належно оформленого реферативного дослідження та публічного представлення його результатів.

На семінарських заняттях передбачається формування навичок застосування правових норм до конкретних обставин. Ситуативні завдання розв'язуються за наступним алгоритмом:

1. Встановлення технічних ознак кіберзлочину.
2. Правова характеристика кіберзлочину.
3. Встановлення алгоритму протидії кіберзлочину.
4. Визначення нормативно-правової бази, необхідної для вирішення конкретної ситуації.

Оскільки формування практичних навичок базується на основі теоретичних знань, на практичних заняттях може здійснюватися поточний контроль у формі тестового опитування.

У процесі семінарського заняття студенти вчаться формулювати свою точку зору, вільно

володіти професійними термінами, логічно викладати матеріал, підбирати докази у підтвердження своїх думок, вчаться публічно виступати, правильно застосовувати норми права на практиці та приймати власні рішення у невизначених ситуаціях.

Питання для обговорення, практичні та індивідуальні завдання для підготовки до семінарських та практичних занять, конкретні вимоги до окремих тем занять подані у відповідних методичних вказівках.

Терміни проведення різних форм занять наведені у схемі вивчення дисципліни.

ВИМОГИ ДО САМОСТІЙНОЇ РОБОТИ СТУДЕНТІВ

Основним завданням самостійної роботи студентів є набуття навичок самостійного опрацювання фахових інформаційних джерел та оволодіння практичними навичками тлумачення і застосування правових норм.

Самостійна робота студентів організовується шляхом видачі індивідуального переліку питань і практичних завдань з кожної теми, які не виносяться на аудиторне опрацювання. Крім того, по деяких темах передбачається написання рефератів, міні-проектів, підготовки презентаційних матеріалів. Обсяг самостійної роботи визначається кількістю годин, передбачених робочою програмою.

ПОЛІТИКА ОЦІНЮВАННЯ ТА АКАДЕМІЧНОЇ ДОБРОЧЕСНОСТІ

Оцінювання здійснюється за 100-бальною шкалою відповідно до **Положення про порядок рейтингового оцінювання знань (освітніх досягнень) здобувачів вищої освіти**

Оцінювання знань студентів з навчальної дисципліни здійснюється шляхом проведення контрольних заходів, які включають:

- *поточний контроль,*
- *модульний контроль,*
- *виконання індивідуального навчально-дослідного завдання.*

Поточний контроль здійснюється під час проведення семінарських занять і має на меті перевірку знань студентів з окремих тем та рівня їх підготовленості до виконання конкретної роботи.

Ключовими методами демонстрації студентами результатів навчання при поточному контролі є:

- усне опитування - передбачає розгорнуту відповідь студента на оцінку; він повинен самостійно пояснити вивчений матеріал, довести наукові положення, навести власні приклади;
- дискусія - обґрунтування власної позиції у вирішенні проблемних питань;
- письмове опитування - з'ясування в письмовій формі ступеня оволодіння студентами знаннями, вміннями та навичками з тем дисципліни, визначення їх якості - правильності, точності, усвідомленості, вміння застосувати знання на практиці;
- тестова перевірка як один із видів письмового опитування - передбачає визначення рівня сформованості знань і вмінь з певної теми дисципліни за допомогою тестів відкритої і закритої форм;

вирішення ситуативних завдань (кейсів) - проводиться з метою об’єктивного з’ясування спроможності студентів застосовувати правові норми, до конкретних життєвих ситуацій, перевірки професійних компетентностей із прийняття рішень в умовах невизначеності.

Ключовими формами демонстрації студентами результатів навчання при поточному контролі є:

- індивідуальна перевірка - проводиться щодо конкретних студентів і має на меті з'ясування рівня засвоєння студентом знань, умінь і навичок, рівня формування професійних компетентностей;
- фронтальна перевірка - форма контролю, що спрямована на з'ясування рівня засвоєння

студентами програмного матеріалу за порівняно короткий час. Вона передбачає короткі відповіді з місця на короткі запитання або письмову роботу;

Модульний контроль проводиться з метою оцінки результатів навчання після закінчення логічно завершеної частини лекційних та семінарських занять з певного змістового модуля.

Основною формою модульного контролю є завдання, які включають як і перевірку теоретичних положень курсу, так і розв'язування практичних завдань.

Індивідуальне навчально-дослідне завдання (ІНДЗ) студенти виконують самостійно під керівництвом викладача. Як правило, індивідуальні завдання виконуються окремо кожним студентом.

ІНДЗ є видом позааудиторної індивідуальної роботи студента навчального, навчально-дослідницького характеру, яке використовується в процесі вивчення програмного матеріалу навчальної дисципліни і завершується оцінюванням. Це завершена теоретична або практична робота в межах навчальної програми курсу, яка виконується на основі знань, вмінь і навичок, отриманих у процесі лекційних, семінарських занять, охоплює тему, декілька тем або зміст навчальної дисципліни в цілому.

Підсумковий контроль проводиться у формі диференційованого заліку.

Підсумковий контроль у формі диференційованого **заліку** - оцінюється на підставі результатів поточного та модульного контролів, захисту ІНДЗ, не передбачаючи обов'язкової присутності студента.

ПРИКЛАД розрахунку підсумкової оцінки, якщо форма підсумкового контролю диференційований залік	**Модуль 1** (поточне опитування)	**Модуль 2** (підсумковий модульний контроль)	**Модуль 3** (ІНДЗ)	**Модуль 4** (екзамен)	**ПІДСУМКОВА ОЦІНКА**
Вагові коефіцієнти, %	70	20	10	–	100
Бали здобувача освіти	80	85	90	–	**82 бали**
Формула розрахунку підсумкової оцінки в балах: 80*0,7+85*0,2+90*0,1=82					

ПОЛІТИКА ЩОДО ВІДВІДУВАННЯ ТА ПЕРЕСКЛАДАННЯ

Здобувач освіти повинен дотримуватись Правил внутрішнього розпорядку Коледжу та відвідувати заняття згідно з розкладом. Очікується, що студенти відвідають усі лекції та семінарські заняття курсу. За об'єктивних причин (наприклад, хвороба, відрядження, участь у науково-дослідницьких заходах, міжнародне стажування навчання можевідбуватись в онлайн формі за погодженням із керівником курсу. Студенти мають інформувати викладача про неможливість відвідувати заняття. У будь-якому випадку студенти зобов'язані дотримуватися термінів, що визначені для виконання усіх видів письмових робіт, які передбачено у межах курсу.

Пропущені заняття та незадовільні оцінки (поточний контроль, ПМК) повинні бути відпрацьовані згідно графіку консультацій викладача. Роботи (ПМК, ІНДЗ), які здаються із порушенням термінів без поважних причин, можуть бути оцінені на нижчу оцінку (до 10 балів).

До початку сесії студенти повинні виконати усі підсумкові контрольні заходи і отримати по кожному з Модулів 1, 2, 3 не менше 60 балів.

ПОЛІТИКА ЩОДО АПЕЛЯЦІЙ

Студент має право оскаржити оцінку, отриману за результатами підсумкового семестрового контролю у формі іспиту (крім незадовільної оцінки). Такі випадки регулюються

Положенням про апеляцію результатів підсумкового контролю знань студентів. Перескладання незадовільних оцінок здійснюється відповідно до Положення про порядок ліквідації академічних заборгованостей здобувачами вищої освіти.

ПОЛІТИКА ЩОДО АКАДЕМІЧНОЇ ДОБРОЧЕСНОСТІ.

У Коледжі академічна доброчесність регулюються Положенням про академічну доброчесність та передбачається за замовчуванням. Це означає, що усі здані роботи є результатом розумової праці студента, їх оригінальними дослідженнями чи міркуваннями. Відсутність посилань на використані джерела, фабрикування джерел, списування (в т.ч. із використанням мобільних пристроїв), втручання в роботу інших студентів становлять, але не обмежують, приклади можливої академічної недоброчесності. Виявлення ознак академічної недоброчесності в письмовій роботі студента є підставою для її незарахування, незалежно від масштабів плагіату чи обману.

Політики Коледжу та документи щодо академічної доброчесності (як інституційного, так і загальнодержавного значення) наведені на сторінці Коледжу АКАДЕМІЧНА ДОБРОЧЕСНІСТЬ.

ЛІТЕРАТУРНІ ТА ІНФОРМАЦІЙНІ ДЖЕРЕЛА КУРСУ

1) Конституція України. URL: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text

2) Закон України «Про інформацію». URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text

3) Закон України «Про науково-технічну інформацію». URL: https://zakon.rada.gov.ua/laws/show/3322-12#Text

4) Закон України «Про захист інформації в інформаційно-комунікаційних системах». URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text

5) Закон України «Про основні засади забезпечення кібербезпеки України». URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text

6) Закон України «Про державну таємницю». URL: https://zakon.rada.gov.ua/laws/show/3855-12#Text

7) Закон України «Про захист персональних даних». URL: https://zakononline.com.ua/documents/show/306885___702634

8) Закон України «Про національну безпеку України». URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text

9) Конвенція про кіберзлочинність, ратифікована Верховною Радою України 07.09.2005. URL: https://zakon.rada.gov.ua/laws/show/994_575#Text

10) Постанова від 19 червня 2019 р. № 518 «Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури» URL: https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF#Text

11) ДСТУ 3396.0-96 Захист інформації Технічний захист інформації. URL: https://tzi.com.ua/downloads/DSTU%203396.0-96.pdf

12) ДСТУ 3396.2-97 Захист інформації Технічний захист інформації. Терміни та визначення. URL: https://tzi.com.ua/downloads/%D0%94%D0%A1%D0%A2%D0%A3%203396.2-97.docx

13) Юридична відповідальність за правопорушення в інформаційній сфері та основи інформаційної деліктології: монографія / І. В. Арістова, О. А. Баранов, О. П. Дзьобань та ін.; за заг. ред. проф. К. І. Бєлякова. Київ:КВІЦ, 2019. 344 с..URL: http://ippi.org.ua/sites/default/files/monografiya_ok_0.pdf

14) Манжай О. В., Манжай І.А. Правові засади захисту інформації: підручник. – Харків : Панов, 2020. – 162 с. URL: http://univd.edu.ua/science-issue/issue/4315

15) Доктрина інформаційної безпеки України: Указ Президента України від 25.02.2017 р. № 47 / Офіційний вісник Президента України. - 2017. - № 5. - С. 15. URL: https://www.president.gov.ua/documents/472017-21374

16) Стратегія кібербезпеки України: Указ Президента України від 26 серпня 2021 року № 447/2021 року. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text

17) Стратегія національної безпеки України : Указ Президента України від 14 вересня 2020 року. URL: https://zakon.rada.gov.ua/laws/show/392/2020#Text

18) Стратегія інформаційної безпеки України, затверджена Указом Президента України від 28 грудня 2021 року № 685/2021. URL: https://www.president.gov.ua/documents/6852021-41069

19) Стратегія воєнної безпеки України: Указ Президента України від 25 березня 2021 року № 121/2021 року. URL: https://zakon.rada.gov.ua/laws/show/121/2021#n8.

20) Кіберзлочинність та електронні докази = Cybercrime and digital evidence : навч. посібник / [Б. М. Головкін, О. І. Денькович, В. В. Луцик, Д. М. Цехан] ; за ред. канд. юрид. наук, доц. Ольги Денькович, д-р права, проф. Габріеле Шмельцер. – Електрон. вид. – Львів : ЛНУ ім. Івана Франка, 2022. – 298 с. URL: https://hdl.handle.net/11300/26072