Затверджено
Завідувач кафедри УКБЗІ _____ С. Легомінова
“ 31 “ серпня 2026 р.

СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ
«ОСНОВИ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ»

Лектор курсу			**Примаченко Діана Володимирівна** викладач кафедри Управління кібербезпекою та захистом інформації		**Контактна інформація лектора (e-mail), сторінка курсу в Classroom**	**e-mail:** d.prymachenko@duikt.edu.ua **сторінка курсу в Classroom–** https://classroom.google.com/c/ODA1Mjg2MDg0MDU2?cjc	
Галузь знань			F «Інформаційні технології»		**Рівень вищої освіти**	Бакалавр	
Спеціальність			F5 «Кібербезпека та захист інформації»		**Семестр**	1	
Освітня програма			«Управління інформаційною та кібернетичною безпекою» «Управління кібербезпекою та захистом інформації»		**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	18	-	18	-	54

АНОТАЦІЯ КУРСУ

Взаємозв’язок у структурно-логічній схемі

Освітні компоненти, які передують вивченню	Базова
Освітні компоненти для яких є базовою	Кваліфікаційна робота. Стандарти інформаційної та кібернетичної безпеки.

Мета курсу:	формування у студентів базових теоретичних знань, необхідних для забезпечення цілісного уявлення щодо управління інформаційною та кібербезпекою.

Компетентності відповідно до освітньої програми

Soft- skills / Загальні компетентності (ЗК)	**Hard-skills / Фахові компетентності (КФ)**
ЗК 1. Здатність застосовувати знання у практичних ситуаціях. **ЗК 2.** Знання та розуміння предметної області та розуміння професії.	**КФ 2.** Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної та кібербезпеки. **КФ 11.** Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-комунікаційних (автоматизованих) систем.

Програмні результати навчання (ПРН)

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

РН 7. Діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, тому числі міжнародних в галузі інформаційної та /або кібербезпеки.			
ОРГАНІЗАЦІЯ НАВЧАННЯ			
Тема, опис теми	**Вид заняття**	**Оцінювання за тему**	**Форми і методи навчання/питання до самостійної роботи**
Тема 1. Концептуальні основи інформаційної та кібербезпеки ***Рекомендовані джерела: 1-3***			
Заняття 1.1 Концептуальні основи інформаційної та кібербезпеки	Лекція 1 6 год		Пояснювально-ілюстративний, лекція-візуалізація, бліц опитування
Заняття 1.2. Основні концепції інформаційної безпеки	Практичне заняття 1.1 2 год	3*	Усне опитування, виконання завдань на практичне застосування знань і вмінь
Заняття 1.3. Основні концепції кібербезпеки	Практичне заняття 1.2 2 год	3*	Усне опитування, виконання завдань на практичне застосування знань і вмінь, тестування
Тема 1. Концептуальні основи інформаційної та кібербезпеки	Самостійна робота 1	4*	Виконання рефератів за обраною темою
Тема 2. Нормативно-правова база в основах інформаційної безпеки та кібербезпеки ***Рекомендовані джерела: 4-6***			
Заняття 2.1 Нормативно-правова база в основах інформаційної безпеки та кібербезпеки	Лекція 2 2 год		Пояснювально-ілюстративний, лекція-візуалізація, бліц опитування
Заняття 2.2. Міжнародні стандарти в основах інформаційної безпеки та кібербезпеки.	Практичне заняття 2.1 2 год	3*	Усне опитування, виконання завдань на практичне застосування знань і вмінь
Заняття 2.3. Національне законодавство в основах інформаційної безпеки та кібербезпеки	Практичне заняття 2.2 2 год	3*	Усне опитування, виконання завдань на практичне застосування знань і вмінь, тестування
Тема 2. Нормативно-правова база в основах інформаційної безпеки та кібербезпеки	Самостійна робота 2	4*	Виконання рефератів за обраною темою
Тема 3. Організаційні аспекти в основах управління інформаційною та кібернетичною безпекою ***Рекомендовані джерела: 7-9***			

Заняття 3.1 Організаційні аспекти в основах управління інформаційною та кібернетичною безпекою	Лекція 3 2 год		Пояснювально-ілюстративний, лекція-візуалізація, бліц опитування
Заняття 3.2. Структура служб безпеки в управлінні інформаційною та кібернетичною безпекою	Практичне заняття 3.1 2 год	3*	Усне опитування, виконання завдань на практичне застосування знань і вмінь
Заняття 3.3. Процеси управління інформаційною та кібернетичною безпекою	Практичне заняття 3.2 2 год	3*	Усне опитування, виконання завдань на практичне застосування знань і вмінь, тестування
Тема 3. Організаційні аспекти в основах управління інформаційною та кібернетичною безпекою	Самостійна робота 3	4*	Виконання рефератів за обраною темою
Тема 4. Технічні засоби у сфері інформаційної та кібербезпеки ***Рекомендовані джерела: 10-12***			
Заняття 4.1 Технічні засоби у сфері інформаційної та кібербезпеки	Лекція 4 2 год		Пояснювально-ілюстративний, лекція-візуалізація, бліц опитування
Заняття 4.2. Засоби захисту інформації в сфері інформаційної та кібербезпеки	Практичне заняття 4.1 2 год	3*	Усне опитування, виконання завдань на практичне застосування знань і вмінь
Заняття 4.3. Системи управління інцидентами у сфері інформаційної та кібербезпеки	Практичне заняття 4.2 2 год	3*	Усне опитування, виконання завдань на практичне застосування знань і вмінь, тестування
Тема 4. Технічні засоби у сфері інформаційної та кібербезпеки	Самостійна робота 4	4*	Виконання рефератів за обраною темою
Тема 5. Людський фактор у концепції інформаційної та кібербезпеки ***Рекомендовані джерела: 13-15***			
Заняття 5.1 Людський фактор у концепції інформаційної та кібербезпеки	Лекція 5 4 год		Пояснювально-ілюстративний, лекція-візуалізація, бліц опитування

Заняття 5.2. Обізнаність персоналу у сфері інформаційної та кібербезпеки	Практичне заняття 5.1 2 год	3*	Усне опитування, виконання завдань на практичне застосування знань і вмінь
Заняття 5.3. Управління ідентифікацією та доступом в концепції інформаційної та кібербезпеки	Практичне заняття 5.2 2 год	3*	Усне опитування, виконання завдань на практичне застосування знань і вмінь, тестування
Тема 5. Людський фактор у концепції інформаційної та кібербезпеки	Самостійна робота 5	4*	Виконання рефератів за обраною темою
Тема 6. Перспектива розвитку управління інформаційною та кібербезпекою ***Рекомендовані джерела:*** ***16-18***			
Заняття 6.1 Перспектива розвитку управління інформаційною та кібербезпекою	Лекція 6 2 год		Пояснювально-ілюстративний, лекція-візуалізація, бліц опитування
Заняття 6.2. Штучний інтелект та машинне навчання в концепції інформаційної та кібербезпеки	Практичне заняття 6.1 2 год	3*	Усне опитування, виконання завдань на практичне застосування знань і вмінь
Заняття 6.3. Хмарні технології у сфері інформаційної та кібербезпеки	Практичне заняття 6.2 2 год	3*	Усне опитування, виконання завдань на практичне застосування знань і вмінь, тестування
Тема 6. Перспектива розвитку управління інформаційною та кібербезпекою	Самостійна робота 6	4*	Виконання рефератів за обраною темою
МАТЕРІАЛЬНО-ТЕХНІЧНЕ ЗАБЕЗПЕЧЕННЯ ДИСЦИПЛІНИ			
Комп‘ютерне обладнання, мережа Інтернет, мультимедійний проєктор.			
ІНФОРМАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ ДИСЦИПЛІНИ			
1. Біленчук П. Д., Обіход Т. В. Кібербезпека і засоби запобігання та протидії кіберзлочинності й кібертероризму. *Часопис Київського університету права*. 2018. № 3. С. 235-239. URL: http://nbuv.gov.ua/UJRN/Chkup_2018_3_54 2. Богуш В.М., Богуш В.В., Бровко В.Д., Настрадін В.П. Основи кіберпростору, кібербезпеки та кіберзахисту. URL: https://jurkniga.ua/contents/osnovi-kiberprostoru-kiberbezpeki-ta-kiberzakhistu.pdf 3. Богуш В.М., Бровко В.Д., Кобус О.С., Козюра В.Д. Технічний захист інформації. Ліра-К : 2022. 4. Гребенюк А.М., Рибальченко Л.В. Основи управління інформаційною безпекою. 2020 5. Костирко Т. М., Т. Д. Корольова Т. Д., Жигалкіна М. С. Основи медіаграмотності. Миколаїв : НУК, 2019.			

6. Троян С.О., Ткачук А.В. Медіаосвіта. Основи медіаграмотності. Умань: ПП Жовтий О.О., 2014.

7. ISO/IEC 27001. Система менеджменту інформаційної безпеки. Женева: Міжнародна організація зі стандартизації, 2015.

8. Криворучко О.В., Звєрєв В.П., Десятко А.М. Кібергігієна. Кібербезпека. Безпека держави: : матеріали наукових семінарів. Київ : КНТЕУ, 2020.

9. Синявський В. В. Управління інформаційною безпекою підприємства. *Economics and management*. 2022. № 4 (2022). С. 61–72. URL: https://doi.org/10.36919/2312-7812.4.2022.61

10. Левченко О. В. Концептуальні основи формування системи забезпечення інформаційної безпеки. *Наука і техніка повітряних сил збройних сил україни*. 2018. № 1(30). С. 7–12. URL: https://doi.org/10.30748/nitps.2018.30.01

11. Подільчак О., Дунаєва Т. Інформаційні методики кібербезпеки як складової інформаційної безпеки під час війни в україні. Наукові інновації та передові технології. 2023. № 13(27). URL: https://doi.org/10.52058/2786-5274-2023-13(27)-329-341

12. Obodiak V., Kotukh Y. Основні виклики урядування у сфері кібербезпеки. Theory and practice of public administration. 2020. Т. 4, № 71. С. 38–46. URL: https://doi.org/10.34213/tp.20.04.05

13. Факас І. Б. Правозастосування у сфері інформаційної безпеки. Вісник Чернівецького факультету Національного університету "Одеська юридична академія". 2016. Вип. № 2. С. 235–243.

14. Веселова Л. Ю. Адміністративно-правові заходи у сфері забезпечення кібербезпеки. Scientific journal of public and private law. 2019. № 6. С. 148–152. URL: https://doi.org/10.32844/2618-1258.2019.6.25

15. Котляров В. Основні підходи у концепції інформаційної безпеки. Актуальні питання у сучасній науці. 2023. № 1(7). URL: https://doi.org/10.52058/2786-6300-2023-1(7)-474-484

16. Наконечний В. С. Стан розвитку управління інформаційною безпекою в світовій практиці та її вплив на економічний розвиток України. Сучасний захист інформації. 2015. № 4. С. 10–15.

17. Чубаєвський В. Методи управління корпоративною інформаційною безпекою. Економіка та суспільство. 2022. № 43. URL: https://doi.org/10.32782/2524-0072/2022-43-49

18. Безштанько В. Цикл впровадження системи управління інформаційною безпекою. *Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні*. 2006. Вип. 2 (13). С. 123–126.

19. Легомінова, С.В., Примаченко, Д.В. Метод оцінювання ризику інформаційної безпеки з урахуванням гібридного впливу. Сучасний захист інформації. 2026. № 2. URL: https://journals.duikt.edu.ua/index.php/dataprotect/article/view/3533/3389

20. Примаченко Д.В., Святська Н.А., Дьячук О.С., Недодай М.Г. Використання можливостей штучного інтелекту у створенні інформаційно-психологічних операцій. Телекомунікаційні та інформаційні технології. 2024. № 2. С. 30-36. URL: https://doi.org/10.31673/2412-4338.2024.024047

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

Маскимальний бал, який може набрати студент – 60. Умовою допуску до підсумкового контролю є набрання студентом 40 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 балу
	• участь у експрес-опитуванні	за кожну правильну відповідь 0,25 балу
	• 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 балу
	• участь у навчальній дискусії, обговоренні ситуаційного завдання	за кожну правильну відповідь 2 бали
	• участь у діловій грі	за кожну участь 1 бал
РУБІЖНЕ ОЦІНЮВАННЯ (КОНТРОЛЬ)	Контроль № 1 "Управління проєктами інформаційної безпеки"	максимальна оцінка 15 балів
	Контроль № 2 "Проєктний аналіз менеджменту інформаційної безпеки"	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. Іспит проходить у письмовій формі.	40 балів

ПІДСУМКОВА ОЦІНКА ЗА ДИСЦИПЛІНУ 100 балів

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. 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 (С)

67-74	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)
60-66	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) *В залікову книжку не проставляється*
1-34	Студент повністю не виконав вимог робочої програми навчальної дисципліни. Його знання на підсумкових етапах навчання є фрагментарними. Студент не допущений до здачі заліку.	**Незадовільний** 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*

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.