Міжнародний гуманітарний університет
Факультет кібербезпеки, програмної інженерії та комп'ютерних наук

Кафедра комп'ютерної інженерії та інноваційних технологій

СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ
Вступ до спеціальності

Галузь знань F Інформаційні технології
Спеціальність F5 Кібербезпека та захист інформації
Назва освітньої програми Кібербезпека
Рівень вищої освіти перший (бакалаврський) рівень

Розробники і викладачі	Контактний тел.	E-mail
зав. кафедри комп'ютерної інженерії та інноваційних технологій к.т.н., доцент **Йона Лариса Григорівна**	+380 67 746 37 77	yonalarysa66@gmail.com

1. АНОТАЦІЯ ДО КУРСУ

Вступ до спеціальності – забезпечує ознайомлення здобувачів з фундаментальними основами професійної діяльності у сфері захисту інформації. Курс охоплює широкий спектр питань, включаючи історію розвитку кібербезпеки, сучасні загрози і виклики інформаційної безпеки, основні напрями професійної діяльності фахівців з кібербезпеки, нормативно-правові аспекти захисту інформації в Україні та світі. Здобувачі отримують уявлення про структуру освітньої програми, перспективи працевлаштування, етичні принципи роботи фахівців у галузі кібербезпеки, а також знайомляться з провідними науковими школами, дослідницькими центрами та компаніями, які формують сучасний ландшафт інформаційної безпеки.

Метою вступу до спеціальності як навчальної дисципліни є формування у здобувачів цілісного уявлення про спеціальність та, її місце в системі сучасних знань та професійної діяльності, а також у розвитку мотивації до подальшого навчання та професійного становлення. Курс спрямований на розвиток базових компетентностей для усвідомленого вибору траєкторії навчання, розуміння відповідальності фахівця з кібербезпеки перед суспільством, формування професійної ідентичності та готовності до безперервного професійного розвитку в умовах динамічного розвитку інформаційних технологій та еволюції кіберзагроз.

ПРЕРЕКВІЗИТИ. Дисципліна вивчається у першому семестрі та не потребує попередніх фахових знань. Вона формує первинні уявлення про спеціальність та є відправною точкою для всього подальшого навчання.

ПОСТРЕКВІЗИТИ. Загальні уявлення про галузь кібербезпеки та основні поняття є підґрунтям для свідомого вивчення всіх наступних фахових дисциплін, зокрема «Захисту інформації в інфокомунікаційних системах та мережах» (ОК 12), «Криптографії та криптоаналізу» (ОК 23), «Комплексних систем захисту інформації» (ОК 24) та «Управління інформаційною та кібербезпекою» (ОК 30).

2. ОЧІКУВАНІ КОМПЕТЕНТНОСТІ, ЯКІ ПЛАНУЄТЬСЯ СФОРМУВАТИ ТА ДОСЯГНЕННЯ ПРОГРАМНИХ РЕЗУЛЬТАТІВ

У процесі реалізації програми дисципліни «Вступ до спеціальності» формуються наступні компетентності із передбачених освітньою програмою:

Інтегральна компетентність

ІК. Здатність розв’язувати складні спеціалізовані задачі та практичні проблеми у галузі кібербезпеки та захисту інформації.

Загальні компетентності (ЗК)

ЗК 1. Здатність застосовувати знання у практичних ситуаціях.

ЗК 2. Знання та розуміння предметної області та розуміння професійної діяльності

ЗК 7. Здатність ухвалювати рішення и діяти дотримуючись принципу неприпустимості корупції та будь-яких інших проявів недоброчесності.

ЗК 8. Здатність зберігати та примножувати моральні, культурні, наукові цінності і досягнення суспільства на основі розуміння історії та закономірностей розвитку предметної області, її місця у загальній системі знань про природу і суспільство та у розвитку суспільства, техніки і технологій, використовувати різні види та форми рухової активності для активного відпочинку та ведения здорового способу життя форми рухової активності для активного відпочинку та ведення здорового способу життя.

Спеціальні (фахові, предметні) компетентності

СК 1. Здатність застосовувати законодавчу та нормативно правову базу, а також державні та міжнародні вимоги, практики і стандарти у професійній діяльності

Навчальна дисципліна «Вступ до спеціальності» забезпечує досягнення програмних результатів навчання (РН), передбачених освітньою програмою:

РН 3. Застосовувати принцип неприпустимості корупції та будь-яких інших проявів недоброчесності у професійній діяльності.

РН 4. Організовувати власну професійну діяльність, обирати і використовувати оптимальні методи та способи розв’язання складних спеціалізованих задач і практичних проблем у професійній діяльності, оцінювати їхню ефективність

РН 5. Аналізувати, аргументувати, приймати рішення при розв’язанні складних спеціалізованих задач і практичних завдань у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення

РН 9. Знати та застосовувати законодавство України та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі кібербезпеки та захисту інформації

РН 19. Вирішувати задачі щодо організації та контролю стану криптографічного захисту інформації, зокрема відповідно до вимог нормативних документів.

3. ОБСЯГ ТА ОЗНАКИ КУРСУ

Загалом		Вид заняття (денне відділення / заочне відділення)			Ознаки курсу		
ЄКТС	**годин**	**Лекційні заняття**	**Практичні заняття**	**Самостійна робота**	**Курс, (рік навчання)**	**Семестр**	**Обов'язкова / вибіркова**
3	90	14 / 6	26 / 2	50 / 82	1	1	Обов'язкова

4. СТРУКТУРА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Назви змістових модулів і тем	Кількість годин							
	денна форма				Заочна форма			
	усього	у тому числі			усього	у тому числі		
		лекц.	прак	сам. роб.		лекц.	прак	сам. роб.
Тема 1. Основні складові підготовки фахівців у сфері кібербезпеки. Здоровий спосіб життя як інструмент професійної ефективності.	12	2	4	6	10		-	10
Тема 2. Академічна доброчесність: етика та відповідальність у навчанні	10	2	2	6	16	2	2	12
Тема 3. Основи інформаційної безпеки: ключові поняття та визначення	14	2	4	8	12	-	-	12
Тема 4. Забезпечення надійного захисту інформації в кіберпросторі. Програма навчання працівників у сфері кібербезпеки (SAT).	15	2	4	9	14	2	-	12
Тема 5. Основні поняття та методи захисту інформації в телекомунікаційних системах.	12	2	4	6	14	2	-	12
Тема 6. Базові поняття про криптографічний захист інформації.	16	2	4	10	12	-	-	12
Тема 7. Соціальна інженерія та методи протидії її шкідливим проявам	11	2	4	5	12	-	-	12
Усього годин	**90**	**14**	**26**	**50**	**90**	**6**	**2**	**82**
ПІДСУМКОВИЙ КОНТРОЛЬ - ЗАЛІК								

5. ТЕХНІЧНЕ Й ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ / ОБЛАДНАННЯ

Здобувачі отримують теми та питання курсу, основну і додаткову літературу, рекомендації, завдання та оцінки за їх виконання як традиційним шляхом, так і з використанням платформ он-лайн навчання на основі інформаційних систем Moodle або Google Classroom.

Виконання практичних робіт та проведення індивідуального тестування, забезпечується за допомогою існуючих в університеті комп'ютерних класів, бібліотеки та платформ он-лайн навчання на основі інформаційних систем Moodle або Google Classroom.

6. САМОСТІЙНА РОБОТА

До самостійної роботи студентів щодо вивчення дисципліни «Вступ до спеціальності» включаються:

1. Знайомство з науковою та навчальною літературою відповідно зазначених у програмі тем.
2. Опрацювання лекційного матеріалу.
3. Підготовка до практичних занять.
4. Консультації з викладачем протягом семестру.
5. Самостійне опрацювання окремих питань навчальної дисципліни.
6. Підготовка та виконання індивідуальних завдань.
7. Підготовка до підсумкового контролю.

Тематика та питання до самостійної підготовки та індивідуальних завдань

№ з/п	Назва теми	Кількість годин	
		денна форма	заочна форма
1	**Тема 1. Основні складові підготовки фахівців у сфері кібербезпеки.** Професійні стандарти та сертифікації в галузі інформаційної безпеки (CISSP, CEH, CompTIA Security+ тощо). Здоровий спосіб життя як інструмент професійної ефективності.	6	10
2	**Тема 2. Академічна доброчесність: етика та відповідальність у навчанні.** Культура академічної доброчесності як основа професійної етики фахівця з кібербезпеки. Кодекси етики професійних організацій в галузі інформаційної безпеки.	6	12
3	**Тема 3. Основи інформаційної безпеки: ключові поняття та визначення.** Вразливості інформаційних систем: технічні, програмні, організаційні, людські. Ризики інформаційної безпеки та методи їх оцінки. Активи інформаційної системи та їх категорії. Інциденти інформаційної безпеки та кіберінциденти.	8	12
4	**Тема 4. Забезпечення надійного захисту інформації в кіберпросторі.** Створення та впровадження програми навчання працівників у сфері кібербезпеки (SAT). Захист кінцевих пристроїв: антивірусне програмне забезпечення, системи контролю пристроїв. Сегментація мережі та принцип найменших привілеїв. Системи управління подіями та інформацією безпеки (SIEM). Моніторинг і аудит інформаційної безпеки. Реагування на інциденти кібербезпеки: виявлення, аналіз, локалізація, відновлення.	9	12

5	**Тема 5. Основні поняття та методи захисту інформації в телекомунікаційних системах.** Основи технічного захисту інформації: методи та інструменти. Системи контролю доступу: фізичні та логічні. Захист від витоку інформації (DLP): канали витоку та методи протидії. Технічні засоби виявлення закладних пристроїв та каналів несанкціонованого отримання інформації. Захист від електромагнітних випромінювань та наведень (TEMPEST). Екранування приміщень та обладнання. Системи знищення інформації на носіях.	6	12
6	**Тема 6. Базові поняття про криптографічний захист інформації.** Призначення криптографічного протоколів: Поняття мережевих протоколів захисту SSL/TLS, IPSec, PGP. Квантова криптографія: перспективи та виклики.	10	12
7	**Тема 7. Соціальна інженерія та методи протидії її шкідливим проявам.** Створення культури безпеки в організації. Відомі приклади атак соціальної інженерії та уроки, які можна з них винести.	5	12
	Всього	**50**	**82**

7. ВИДИ ТА МЕТОДИ КОНТРОЛЮ

Види контролю	**Складові оцінювання**	
	Для екзамену	**Для заліку**
поточний контроль, який здійснюється у ході: проведення практичних (лабораторних) занять, виконання самостійної роботи, індивідуальних завдань, дослідна робота здобувача тощо.	**50%**	**100%**
підсумковий контроль	**50%**	

Методи діагностики знань (контролю)	фронтальне опитування; наукова доповідь, реферати, усне повідомлення, індивідуальне опитування; розв`язання практичних завдань, залік.

8. ОЦІНЮВАННЯ ЗДОБУВАЧІВ ВИЩОЇ ТА ФАХОВОЇ ПЕРДВИЩОЇ ОСВІТИ ЗА НАВЧАЛЬНУ ДИСЦИПЛІНУ У МІЖНАРОДНОМУ ГУМАНІТАРНОМУ УНІВЕРСИТЕТІ

(*поточний контроль, підсумковий контроль, загальний результат оцінювання)*

ЗАЛІК

Поточний контроль			
Види роботи	**Планові терміни виконання**	**Форми контролю та звітності**	**Максимальний відсоток оцінювання**
Систематичність і активність роботи на практичних (лабораторних) заняттях			
1.1. Підготовка до практичних (лабораторних) занять	Відповідно до робочої програми та розкладу занять	Перевірка обсягу та якості засвоєного матеріалу під час практичних (лабораторних) занять	**60**
Виконання завдань для самостійного опрацювання			
1.2. Індивідуальне тестування, завдання, підготовка реферату (есе) за заданою тематикою	Відповідно до робочої програми та розкладу занять	Розгляд відповідного матеріалу під час аудиторних занять або ІКР[1], перевірка конспектів навчальних текстів тощо	**20**
Виконання індивідуальних завдань, дослідна робота здобувача			
1.3. Інші види індивідуальних завдань, в т.ч. підготовка наукових публікацій, участь у роботі круглих столів, конференцій тощо.	Відповідно до робочої програми та розкладу занять	Обговорення результатів проведеної роботи під час аудиторних занять, наукових конференцій та круглих столів.	**20**
Разом балів за поточний контроль			**100**
Загальний результат оцінювання			**100**

[1] Індивідуально-консультативна робота викладача зі здобувачами

Поточний контроль знань здобувачів освіти при формі контролю **залік** (максимум 100 балів) оцінюється за шкалою *(«2», «3», «4», «5»)*, з обов'язковим переведенням балів за кожний вид роботи таким чином:

- за підготовку до аудиторних занять (максимум 60 балів) здобувачу освіти необхідно мати не менше 1/2 оцінок від загальної кількості практичних (лабораторних) занять, для переводу балів за підготовку до аудиторних занять середньоарифметична оцінка множиться на коефіцієнт 12;
- за виконання завдань для самостійного опрацювання (тестування, завдання, підготовка реферату (есе) за заданою тематикою) (максимум 20 балів) здобувачу освіти необхідно мати не менше 1/2 оцінок від загальної кількості програмного матеріалу, що виноситься на самостійне вивчення, для переводу зазначених балів середньоарифметична оцінка множиться на коефіцієнт 4;
- за інші види індивідуальних завдань, в т.ч. підготовку наукових публікацій, участь у роботі круглих столів, конференцій тощо (максимум 20- балів) здобувачу освіти необхідно мати не менше 1/2 оцінок від загальної кількості інших видів індивідуальних завдань, для переводу балів за підготовку до аудиторних занять середньоарифметична оцінка множиться на коефіцієнт 4.

КРИТЕРІЇ ОЦІНЮВАННЯ ЗА ПОТОЧНИЙ КОНТРОЛЬ

- «2»- виставляється за неправильну відповідь (письмову роботу), яка не відповідає змісту теми та свідчить про нерозуміння її основних положень;
- «3» -виставляється за відповідь (письмову роботу), яка відповідає змісту теми, але є неповною і неточною у визначенні понять, свідчить про неповне розуміння основних положень навчального матеріалу, свідчить про те, що знання студента мають фрагментарний, поверховий характер;
- «4» - оцінюється правильна і обґрунтована відповідь (письмова робота), з якої видно, що студент знає й розуміє теоретичний матеріал в обсязі навчальної теми, володіє необхідними навичками, не допускає суттєвих помилок.
- «5» - оцінюється повна, правильна, ґрунтовна відповідь (письмова робота) на запитання теми, що передбачає логічність і послідовність викладу матеріалу, володіння термінологією, показує вміння повно й глибоко використовувати теоретичні знання в практичній площині.

9. КРИТЕРІЇ ЗАГАЛЬНИХ РЕЗУЛЬТАТІВ ОЦІНЮВАННЯ ЗНАНЬ ЗДОБУВАЧІВ
(для екзамену / заліку)

Рівень знань оцінюється:

- «відмінно» / «зараховано» A - від 90 до 100 балів. Студент виявляє особливі творчі здібності, вміє самостійно знаходити та опрацьовувати необхідну інформацію, демонструє знання матеріалу, проводить узагальнення і висновки. Був присутній на лекціях та семінарських заняттях, під час яких давав вичерпні, обґрунтовані, теоретично і практично правильні відповіді, має конспект з виконаними завданнями до самостійної роботи, презентував реферат (есе) за заданою тематикою, проявляє активність і творчість у науково-дослідній роботі;
- «добре» / «зараховано» B - від 82 до 89 балів. Студент володіє знаннями матеріалу, але допускає незначні помилки у формуванні термінів, категорій, проте за допомогою викладача швидко орієнтується і знаходить правильні відповіді. Був присутній на лекціях та семінарських заняттях, має конспект з виконаними завданнями до самостійної роботи, презентував реферат (есе) за заданою тематикою, проявляє активність і творчість у науково-дослідній роботі;
- «добре» / «зараховано» C - від 74 до 81 балів. Студент відтворює значну частину теоретичного матеріалу, виявляє знання і розуміння основних положень, з допомогою викладача може аналізувати навчальний матеріал, але дає недостатньо обґрунтовані, невичерпні відповіді,

допускає помилки. При цьому враховується наявність конспекту з виконаними завданнями до самостійної роботи, реферату та активність у науково-дослідній роботі;

- «задовільно» / «зараховано» D - від 64 до 73 балів. Студент був присутній не на всіх лекціях та семінарських заняттях, володіє навчальним матеріалом на середньому рівні, допускає помилки, серед яких є значна кількість суттєвих. При цьому враховується наявність конспекту з виконаними завданнями до самостійної роботи, рефератів (есе);
- «задовільно» / «зараховано» E - від 60 до 63 балів. Студент був присутній не на всіх лекціях та семінарських заняттях, володіє навчальним матеріалом на рівні, вищому за початковий, значну частину його відтворює на репродуктивному рівні, на всі запитання дає необґрунтовані, невичерпні відповіді, допускає помилки, має неповний конспект з завданнями до самостійної роботи.
- «незадовільно з можливістю повторного складання» / «не зараховано» FX – від 35 до 59 балів. Студент володіє матеріалом на рівні окремих фрагментів, що становлять незначну частину навчального матеріалу.
- «незадовільно з обов'язковим повторним вивченням дисципліни» / «не зараховано» F – від 0 до 34 балів. Студент не володіє навчальним матеріалом.

ТАБЛИЦЯ ВІДПОВІДНОСТІ ЗАГАЛЬНИХ РЕЗУЛЬТАТІВ ОЦІНЮВАННЯ ЗНАНЬ ЗА РІЗНИМИ ШКАЛАМИ

100-бальною шкалою	Шкала за ECTS	За національною шкалою	
		екзамен	залік
90-100	A	Відмінно	Зараховано
82-89	B	Добре	
74-81	C		
64-73	D	Задовільно	
60-63	E		
35-59	Fx	Незадовільно	Не зараховано
1-34	F		

10. ДОТРИМАННЯ ВИМОГ АКАДЕМІЧНОЇ ДОБРОЧЕСНОСТІ

Викладання та засвоєння навчальної дисципліни передбачає неухильне дотримання вимог академічної доброчесності, яка регулюється Законом України "Про освіту" (Відомості Верховної Ради (ВВР), 2014, № 37-38, ст.2004), «Методичними рекомендаціями для закладів вищої освіти з підтримки принципів академічної доброчесності» (Лист МОН № 1/9-650 від 23.10.18 року), іншими нормативними документами. Зокрема, основні засади дотримання академічної доброчесності визначено у «Положенні про академічну доброчесність у Міжнародному гуманітарному університеті», «Кодексі академічної доброчесності Міжнародного гуманітарного університету» та «Інструкції щодо процедури технічної перевірки на наявність текстових запозичень (академічного плагіату)», затвердженої наказом МГУ від 03.05.2024 р., № 708а.

Відповідно до ст.42 Закону України "Про освіту" академічна доброчесність - це сукупність етичних принципів та визначених законом правил, якими мають керуватися учасники освітнього процесу під час навчання, викладання та провадження наукової (творчої) діяльності з метою забезпечення довіри до результатів навчання та/або наукових (творчих) досягнень.

Дотримання академічної доброчесності передбачає:

- самостійне виконання навчальних завдань, завдань поточного та підсумкового контролю результатів навчання (для осіб з

особливими освітніми потребами ця вимога застосовується з урахуванням їхніх індивідуальних потреб і можливостей);

- посилання на джерела інформації у разі використання ідей, розробок, тверджень, відомостей;
- дотримання норм законодавства про авторське право і суміжні права;
- надання достовірної інформації про результати власної навчальної (наукової, творчої) діяльності, використані методики досліджень і джерела інформації.

11. РЕКОМЕНДОВАНА ЛІТЕРАТУРА

Основна

1. Онацький О.В., Йона Л.Г., Бєлова Ю.В. Криптографічний захист інформації: Навч.посібник. - Одеса: Одеса : «Астропринт» 2023. 252с. https://surl.li/onvhbl
2. Горбенко Ю. І., Горбенко І. Д. Інфраструктури відкритих ключів. Системи ЕЦП. Теорія та практика : монографія. Харків : Форт, 2010. 593 с.
3. Домарєв В. В. Безпека інформаційних технологій. Системний підхід. Київ : ТІД «ДС», 2004. 992 с.
4. Есін В. І., Кузнєцов О. О., Сорока Л. С. Основи кібербезпеки : підручник. Київ : Освіта України, 2020. 416 с.
5. Корченко О. Г. Побудова систем захисту інформації на базі міжнародних стандартів : навчальний посібник. Київ : ТОВ «НВП «Інтертехнодрук», 2010. 200 с.
6. Кузнецов О. О., Довгий С. О., Король О. Г. Безпека інформаційних технологій : підручник. Київ : Видавнича група BHV, 2008. 544 с.
7. Лахно В. А. Кібербезпека та кіберзахист критичної інфраструктури держави : монографія. Київ : НАУ, 2015. 240 с.
8. Ткач Ю. М., Ільєнко А. В., Ільєнко С. С. Інформаційна безпека : підручник. Київ : Центр учбової літератури, 2018. 438 с.
9. Шелест М. Є., Skladannyi P. M. Основи кібербезпеки : навчальний посібник. Маріуполь : ПДТУ, 2019. 156 с.
10. Яремчук Ю. Є., Брежнєва К. С. Основи інформаційної безпеки : навчальний посібник. Київ : КПІ ім. Ігоря Сікорського, 2017. 240 с.
11. Юдін О. К., Корченко О. Г., Конахович Г. Ф. Захист інформації в мережах передачі даних : навчальний посібник. Київ : ДУТ, 2009. 716 с.

Допоміжна

1. Anderson R. Security Engineering: A Guide to Building Dependable Distributed Systems. 3rd ed. Indianapolis : Wiley, 2020. 1232 p.
2. Bishop M. Computer Security: Art and Science. 2nd ed. Boston : Addison-Wesley, 2018. 1440 p.
3. Hadnagy Ch. Social Engineering: The Science of Human Hacking. 2nd ed. Indianapolis : Wiley, 2018. 320 p.
4. Schneier B. Applied Cryptography: Protocols, Algorithms and Source Code in C. 20th Anniversary Edition. Indianapolis : Wiley, 2015. 784 p.
5. Stallings W., Brown L. Computer Security: Principles and Practice. 4th ed. Pearson, 2017. 800 p.
6. Whitman M. E., Mattord H. J. Principles of Information Security. 7th ed. Boston : Cengage Learning, 2021. 688 p.

Інформаційні ресурси

1. Державна служба спеціального зв'язку та захисту інформації України. URL: https://cip.gov.ua/.

2. Департамент кіберполіції Національної поліції України. URL: https://cyberpolice.gov.ua/ .
3. CERT-UA – Урядова команда реагування на комп'ютерні надзвичайні події України. URL: https://cert.gov.ua/ .
4. Національний координаційний центр кібербезпеки при РНБО України. URL: https://www.rnbo.gov.ua/ua/Aparat/structural-units/NKCK.html .
5. NIST Cybersecurity Framework. National Institute of Standards and Technology. URL: https://www.nist.gov/cyberframework.
6. ENISA – European Union Agency for Cybersecurity. URL: https://www.enisa.europa.eu/.
7. OWASP – Open Web Application Security Project. URL: https://owasp.org/.
8. SANS Institute – Cybersecurity Training and Certification. URL: https://www.sans.org/.
9. Krebs on Security – Cybersecurity News and Investigation. URL: https://krebsonsecurity.com/.