Міжнародний гуманітарний університет
Факультет Кібербезпеки, програмної інженерії та комп'ютерних наук
Кафедра Комп'ютерної інженерії та інноваційних технологій

СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Інформаційна безпека інноваційної діяльності

Галузь знань 12 «Інформаційні технології»
Спеціальність 125 «Кібербезпека та захист інформації»
Назва освітньої програми Кібербезпека
Рівень вищої освіти другий (магістерський) рівень

Розробники і викладачі	Контактний тел.	E-mail
Професор кафедри Комп'ютерної інженерії та інноваційних технологій **Радівілова Тамара Анатоліївна**	+380951609153	tamara.radivilova@gmail.com
Доцент кафедри Комп'ютерної інженерії та інноваційних технологій **Йона Лариса Григорівна**	+380677463777	yonalarysa66@gmail.com

1. АНОТАЦІЯ ДО КУРСУ

Інформаційна безпека інноваційної діяльності є складовою частиною навчального процесу у підготовці фахівців зі спеціальності 125 «Кібербезпека та захист інформації», а також обов'язковим компонентом освітньої програми для здобуття освітнього рівня «магістр» та має на меті формування у здобувачів уявлення про проблеми захисту інформації від порушення її конфіденційності, цілісності та доступності; надання знань фахівцям з сучасних методів захисту інформаційного середовища інноваційних підприємств, тенденцій в галузі захисту інноваційної діяльності, аналіз загроз та ризиків витоку конфіденційної інформації для забезпечення конкурентних переваг інноваційних підприємств, особливостей формування і роботи систем інформаційної безпеки в інноваційних підприємствах та організаціях.

Метою викладання навчальної дисципліни Інформаційна безпека інноваційної діяльності є забезпечення здобувачів знаннями з питань попередження, прогнозування та мінімізації втрат від несанкціонованого доступу до конфіденційної інформації при інноваційній діяльності у системах комунікацій з урахуванням сучасного стану та перспективних напрямів розвитку систем та технологій захисту інформації;

сформувати у здобувача здатність досліджувати, розробляти, впроваджувати та супроводжувати методи і засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності та критичної інфраструктури, в інформаційних системах, а також здатність оцінювати ефективність їх використання, згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.

Передумови для вивчення дисципліни – знання і вміння, отримані студентом при вивченні навчальних дисциплін бакалаврської підготовки.

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

Інтегральна компетентність

ІК. Здатність особи розв'язувати задачі дослідницького та/або інноваційного характеру у сфері інформаційної безпеки та/або кібербезпеки.

Загальні компетентності

КЗ1. Здатність застосовувати знання у практичних ситуаціях.

КЗ2. Здатність проводити дослідження на відповідному рівні.

Фахові компетентності

КФ1. Здатність обґрунтовано застосовувати, інтегрувати, розробляти та удосконалювати сучасні інформаційні технології, фізичні та математичні моделі, а також технології створення та використання прикладного і спеціалізованого програмного забезпечення для вирішення професійних задач у сфері інформаційної безпеки та/або кібербезпеки.

КФ3. Здатність досліджувати, розробляти і супроводжувати методи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.

КФ8. Здатність досліджувати, розробляти, впроваджувати та супроводжувати методи і засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності та критичної інфраструктури, в інформаційних системах, а також здатність оцінювати ефективність їх використання, згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.

Програмні результати навчання

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.

РН3. Провадити дослідницьку та/або інноваційну діяльність в сфері інформаційної безпеки та/або кібербезпеки, а також в сфері технічного та криптографічного захисту інформації у кіберпросторі.

РН8. Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.

РН9. Аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації на базі стратегії і політики інформаційної безпеки.

РН10. Забезпечувати безперервність бізнес/операційних процесів, а також виявляти уразливості інформаційних систем та ресурсів, аналізувати та оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації.

РН11. Аналізувати, контролювати та забезпечувати ефективне функціонування системи управління доступом до інформаційних

ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки та/або кібербезпеки організації.

РН13. Досліджувати, розробляти, впроваджувати та використовувати методи та засоби криптографічного та технічного захисту інформації бізнес/операційних процесів, а також аналізувати і надавати оцінку ефективності їх використання в інформаційних системах, на об'єктах інформаційної діяльності та критичної інфраструктури.

РН14. Аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес\операційних процесів у сфері інформаційної та\або кібербезпеки в цілому.

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.

РН17. Мати навички автономного і самостійного навчання у сфері інформаційної безпеки та/або кібербезпеки і дотичних галузей знань, аналізувати власні освітні потреби та об'єктивно оцінювати результати навчання.

РН21. Використовувати методи натурного, фізичного і комп'ютерного моделювання для дослідження процесів, які стосуються інформаційної безпеки та/або кібербезпеки.

РН22. Планувати та виконувати експериментальні і теоретичні дослідження, висувати і перевіряти гіпотези, обирати для цього придатні методи та інструменти, здійснювати статистичну обробку даних, оцінювати достовірність результатів досліджень, аргументувати висновки.

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**
4	120	22 / 6	22 / 6	76 / 108	1	1 /	Обов'язкова

4. СТРУКТУРА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ
5.

Назви змістових модулів і тем	**Кількість годин**							
	денна форма				**Заочна форма**			
	усього	**у тому числі**			**усього**	**у тому числі**		
		лекц.	**практ.**	**сам. роб.**		**лекц.**	**прак**	**сам. роб.**
Тема 1 **Основні поняття та визначення.** Інноваційні процеси та їх класифікація. Стан сучасної кібербезпеки та шляхи розвитку на майбутнє. Конкурентні переваги при інноваційній діяльності.	10	2		8	10	2		8

Тема 2. **Загрози та ризики витоку конфіденційної інформації.** Загрози інформаційної безпеки держави в соціальних мережах. Аналіз проблеми оперативного виявлення і реагування на інциденти кібербезпеки в телекомунікаціях.	10	2	2	6	10		2	8
Тема 3. **Сучасні тенденції в галузі захисту інформації інноваційного підприємництва.** Комерційна інформація та комерційна таємниця.	10	2	2	6	10			10
Тема 4. **Структура і завдання політики інформаційної безпеки.** Кадрова політика, моніторинг і контроль. Захист від недоброчесної конкуренції та шпигунства. Створення та впровадження програми навчання працівників у сфері кібербезпеки (SAT).	10		2	8	10		2	8
Тема 5. **Соціальна інженерія**. Загрози кіберсистемам. Використання методів соціальної інженерії для захисту інноваційної діяльності від кібератак.	10	2	2	6	10			10
Тема 6. **Управління контролем доступу.** Основна функція управління контролю доступом.	10	2	2	6	10	2		8
Тема 7. **Перспективи систем забезпечення інформаційної безпеки кіберпростору**. Кібербезпека комунікаційних систем і мереж.	10	2	2	6	10			10
Тема 8. **Засоби захисту від витоку інформації в Інтернет.** Програмно-апаратні системи шифрування, брандмауери, системи попередження вторгнення.	10	2	2	6	10		2	8
Тема 9**. Протокол захисту електронних транзакцій TLS**. Порівняння версій протоколів TLS 2.0 та 3.0	10	2	2	6	10	2		8
Тема 10. **Захист електронної пошти.** Боротьба зі спамом та фішингом.	10	2	2	6	10			10
Тема 11. **Безпека мережі з програмованими параметрами SDN.**	10	2	2	6	10			10
Тема 12. **Додаткові методи підвищення безпеки мережі ІКТ.**	10	2	2	6	10			10
Усього годин	**120**	**22**	**22**	**76**	**120**	**6**	**6**	**108**
ПІДСУМКОВИЙ КОНТРОЛЬ – залік								

5. ТЕХНІЧНЕ Й ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ / ОБЛАДНАННЯ

Здобувачі отримують теми та питання дисципліни, основну і додаткову літературу, рекомендації, завдання та оцінки за їх виконання.

6. САМОСТІЙНА РОБОТА

До самостійної роботи студентів щодо вивчення дисципліни «Інформаційна безпека інноваційної діяльності» включаються:

1. Знайомство з науковою та навчальною літературою відповідно зазначених у програмі тем.
2. Опрацювання теоретичного матеріалу, здобутого під час семестру.
3. Виконання практичних та індивідуальних завдань, сформованих викладачем.
4. Консультації з викладачем протягом семестру.
5. Самостійне опрацювання окремих питань навчальної дисципліни.
6. Підготовка та виконання індивідуальних завдань.
7. Підготовка до підсумкового контролю знань.

Тематика та питання до самостійної підготовки та індивідуальних завдань

№ з/п	Назва теми	Кількість годин	
		денна форма	заочна форма
1	**Тема 1.** Вивчення Положення закону «Про національну безпеку України»	8	8
2	**Тема 2.** Вивчення Положення закону України «Про інноваційну діяльність» .	6	8
3	**Тема 3.** Дослідження впливу витоку конфіденційної інформації на стан розвитку сучасного підприємсива.	6	10
4	**Тема 4.** Дослідження методів захисту від недоброчесної конкуренції та шпигунства**.** Дослідження програми навчання працівників у сфері кібербезпеки (SAT).	8	8
5	**Тема 5.** Класифікація кіберзагроз та види кібератак.	6	10
6	**Тема 6.** Дослідження мережевих систем виявлення вторгнень.	6	8
7	**Тема 7.** Дослідження комплексного підходу виявлення вторгнень заснований на аналізі трафіка.	6	10
8	**Тема 8.** Дослідження порівняльної характеристики сучасних криптосистем, що використовуються для захисту конфіденційної інформації**.**	6	8
9	**Тема 9.** Дослідження протоколу захисту електронних транзакцій 3D-Secur для додаткового кроку автентифікації**.**	6	8
10	**Тема 10.** Класифікація загроз та правила поведінки працівників в корпоративній мережі.	6	10
11	**Тема 11.** Дослідження Віртуальних спільнот, як суб’єктів інформаційної безпеки Держави.	6	10
12	**Тема 12.** Дослідження моделі забезпечення безпеки в комп’ютерних системах.	6	10
	Всього	**76**	**108**

7. ВИДИ ТА МЕТОДИ КОНТРОЛЮ

Види контролю	Складові оцінювання
Поточний контроль, який здійснюється під час проведення практичних занять, виконання індивідуального завдання, проведення консультацій та відпрацювання пропущених здобувачем занять.	**50%**
Підсумковий контроль, який здійснюється під час проведення екзамену.	**50%**
Методи діагностики знань (контролю)	фронтальне опитування; наукова доповідь, тези доповіді, наукова стаття, індивідуальне опитування, тестування, екзамен.

8. ОЦІНЮВАННЯ ПОТОЧНОЇ, САМОСТІЙНОЇ ТА ІНДИВІДУАЛЬНОЇ РОБОТИ СТУДЕНТІВ З ПІДСУМКОВИМ КОНТРОЛЕМ У ФОРМІ ЕКЗАМЕНУ.

Денна та заочна форми навчання			
Поточний контроль			
Види роботи	**Планові терміни виконання**	**Форми контролю та звітності**	**Максимальний відсоток оцінювання**
Систематичність і активність роботи на базі практики			
1.1. Підготовка до практичних занять.	Відповідно до робочої програми та розкладу занять	Перевірка обсягу та якості засвоєного матеріалу під час практичних занять	**25**
Виконання завдань для самостійного опрацювання			
1.2. Підготовка програмного матеріалу (тем,питань) для самостійного вивчення	Відповідно до робочої програми та розкладу занять	Розгляд відповідного матеріалу під час аудиторних занять або індивідуально-консультативна робота (ІКР) викладача зі здобувачами.	**10**
Виконання індивідуальних завдань (науково-дослідна робота студента)			
1.3. Підготовка реферату за заданою тематикою.	Відповідно до розкладу занять і графіку ІКР	Обговорення (захист) матеріалів реферату.	**10**
1.4. Інші види індивідуальних завдань, зокрема, підготовка наукових публікацій, участь у роботі круглих столів, конференцій тощо.	Відповідно до розкладу занять і графіку ІКР	Обговорення результатів проведеної роботи під час аудиторних занять, наукових конференцій та круглих столів.	**5**
Разом балів за поточний контроль			**50**
*Підсумковий контроль – **екзамен***			**50**
Всього балів			**100**

Заочна форма навчання

9. КРИТЕРІЇ ПІДСУМКОВОЇ ОЦІНКИ ЗНАНЬ СТУДЕНТІВ
(для іспиту / заліку)

Рівень знань оцінюється:

- «відмінно» / «зараховано» A - від 90 до 100 балів. Здобувач виявляє особливі творчі здібності, вміє самостійно знаходити та опрацьовувати необхідну інформацію, демонструє знання матеріалу, проводить узагальнення і висновки. Був присутній на лекціях та практичних заняттях, під час яких давав вичерпні, обґрунтовані, теоретично і практично правильні відповіді, має конспект з виконаними завданнями до самостійної роботи, презентував реферат за заданою тематикою, проявляє активність і творчість у науково-дослідній роботі;

- «добре» / «зараховано» B - від 82 до 89 балів. Здобувач 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 практичних заняттях, має конспект з виконаними завданнями до самостійної роботи, презентував реферат за заданою тематикою, проявляє активність і творчість у науково-дослідній роботі;

- «добре» / «зараховано» C - від 74 до 81 балів. Здобувач 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. Здобувач був присутній не на всіх лекціях та практичних 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;

- «задовільно» / «зараховано» E - від 60 до 63 балів. Здобувач був присутній не на всіх лекціях та практичних 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 результатів контролю знань за різними шкалами

100-бальною шкалою	Шкала за ECTS	За національною шкалою	
		екзамен	залік
90-100 (10-12)	A	Відмінно	Зараховано
82-89 (8-9)	B	Добре	
74-81(6-7)	C		
64-73 (5)	D	Задовільно	
60-63 (4)	E		
35-59 (3)	Fx	Незадовільно	Не зараховано
1-34 (2)	F		

10. РЕКОМЕНДОВАНА ЛІТЕРАТУРА

Основна

1 . Кононович В.Г., Стайкуца С.В., Берднiков О.М., Севастєєв Є.О., Швець О.В. Інформаційна безпека інноваційної діяльності в інфокомунікаціях : підручник та дистанційний практикум для освітньо-професійної підготовки магістрів за спеціальністю 125 «Кібербезпека та захист інформації» . За ред. д.т.н., проф. В.В.Корчинського. Передмова д.т.н., проф. Є. В. Василіу. Післямова д.т.н., проф. С.О.Гнатюка. - Вид.2-ге, випр., доп. - Одеса: Астропринт, 2023. 380 с. (для аудиторного та дистанційного навчання, мова: укр., англ).

Допоміжна

2. Криптографічний захист інформації: Навч. посіб./ Йона Л.Г., Онацький О.В., Бєлова Ю.В.. - Одеса: ДУІТЗ, 2023. – 250 с., ел.вар.

Інформаційні ресурси

1 Наказ МОН № 332 від 18.03.2021 року Про затвердження стандарту вищої освіти за спеціальністю 125 «Кібербезпека» для другого (магістерського) рівня вищої освіти. URL: https://osvita.ua/legislation/Vishya_osvita.
2 Національна бібліотека України ім. В.І. Вернадського. URL: http://www.nbuv.gov.ua.
3 Портал кіберполіції України. URL: https://cyberpolice.gov.ua/
4 Портал урядової команди реагування на комп'ютерні надзвичайні події України (CERT-UA). URL: https://cert.gov.ua/
5 Radivilova, L. Kirichenko, M. Tawalbeh, P. Zinchenko, V. Bulakh, «Балансування самоподібного трафіку в мережних системах виявлення вторгнень », Кібербезпека: освіта, наука, техніка, Том. 3, вип. 7, с. 17-30, Бер 2020. DOI: https://doi.org/10.28925/2663-4023.2020.7.1730 (Радівілова, Л. Кириченко, М. Тавалбе, П. Зінченко, В. Булах, «Балансування самоподібного трафіку в мережевих системах виявлення вторгнень», Кібербезпека: освіта, наука, техніка, Том. 3, вип. 7, с. 17-30, Бер 2020. DOI: https://doi.org/10.28925/2663-4023.2020.7.1730)
6 4. Радівілова Т.А., Ільков А.А., Тавалбех М.Х. Комплексний метод виявлення вторгнень заснований на статистичному та динамічному підходах аналізу трафіка. Радіоелектроніка та інформатика. № 01. 2020. С. С.17-25.
7 Комплекс навчально-методичного забезпечення навчальної дисципліни "Захист систем електронної комерції та мультисервісних систем", освітньо-кваліфікаційний рівень бакалавр для спеціальності 125 - Кібербезпека [Електронний ресурс] : освітня програма підготовки "Управління інформаційною безпекою" / ХНУРЕ ; розроб. Т.А. Радівілова. – Харків, 2019. – 397 с. - pdf / 13,03 Mb.