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 17 Електроніка та телекомунікації
Спеціальність 172 Телекомунікації та радіотехніка
Назва освітньої програми Комп'ютерні мережі та Інтернет
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 172 Телекомунікації та радіотехніка, 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

У процесі реалізації програми дисципліни «Інформаційна безпека інноваційної діяльності» формуються наступні компетентності та результати навчання із передбачених освітньо-професійною програмою «Комп'ютерні мережі та Інтернет» зі спеціальності 172 Телекомунікації та радіотехніка.

Інтегральна компетентність (ІК)	
ІК-1	Здатність розв'язувати складні спеціалізовані задачі та практичні проблеми у професійній діяльності спрямованій на створення умов та засобів для обміну інформацією, в тому числі комп'ютерних мереж та Інтернет, технічних засобів й програмних додатків, які забезпечують її надійне та якісне передавання, оброблення та зберігання, що передбачає застосування певних методів відповідної науки і характеризується комплексністю та невизначеністю умов.
Загальні компетентності (ЗК)	
ЗК-1	Здатність до абстрактного мислення, аналізу та синтезу
ЗК-2	Здатність застосовувати знання у практичних ситуаціях
ЗК-3	Знання та розуміння предметної області та розуміння професійної діяльності
Спеціальні (фахові) компетентності	
СК-4	Здатність розв'язувати задачі забезпечення надійності, живучості, завадозахищеності, інформаційної безпеки та пропускної здатності телекомунікаційних і радіотехнічних систем з урахуванням економічних, правових, безпекових та інших аспектів.
СК-6	Здатність захищати інтелектуальну власність, дотримуватися правових і етичних норм з питань інтелектуальної власності.
СК-11	Здатність реагувати на порушення рівня інформаційної безпеки в мережі, налаштовувати засоби мережної безпеки та термінального, комутаційного та серверного обладнання.
Програмні результати навчання (ПРН)	
ПРН-1	Організовувати власну професійну, науково-дослідницьку та інноваційну діяльність на основі принципів системного підходу та методології наукових досліджень.
ПРН-2	Проводити наукові дослідження і виконувати проекти на умовах результативного співробітництва у колективі з врахуванням соціальних і морально-етичних норм.
ПРН-9	Забезпечувати надійність, живучість, завадозахищеність, інформаційну безпеку та пропускну здатність телекомунікаційних і радіотехнічних систем.

ПРН-13	Здатність здійснювати пошук інформації у науково-технічній та довідковій літературі, патентах, базах даних, інших джерелах, аналізувати і критично оцінювати цю інформацію з метою детального вивчення і дослідження комп'ютерних мереж та Інтернет.

3. ОБСЯГ ТА ОЗНАКИ КУРСУ

Загалом		**Вид заняття** (денна / заочна форма навчання)			**Ознаки курсу**		
ЄКТС	**годин**	**Лекційні заняття**	**Практичні заняття**	**Самостійна робота**	**Курс, (рік навчання)**	**Семестр**	**Обов'язкова / вибіркова**
4	120	28 / 6	28 / 6	64 / 108	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.	**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.	8	2	2	4	9	2		7
Тема 2. **Загрози та ризики витоку конфіденційної інформації.** Аналіз проблеми оперативного виявлення і реагування на інциденти кібербезпеки в телекомунікаціях.	8	2	2	4	9	2		7
Тема 3. **Сучасні тенденції в галузі захисту інформації інноваційного підприємництва.** Комерційна інформація та комерційна таємниця.	8	2	2	4	9	2		7
Тема 4. **Структура і завдання політики інформаційної безпеки.** Кадрова політика, моніторинг і контроль. Захист від недоброчесної конкуренції та шпигунства.	8	2	2	4	9		2	7
Тема 5. **Соціальна інженерія**. Загрози кіберсистемам. Використання методів соціальної інженерії для захисту інноваційної діяльності від кібератак.	8	2	2	4	7			7
Тема 6. **Управління контролем доступу.** Основна функція управління	10	2	2	6	12		2	10

контролю доступом.								
Тема 7. **Перспективи систем забезпечення інформаційної безпеки кіберпростору**. Кібербезпека комунікаційних систем і мереж.	10	2	2	6	7			7
Тема 8. **Засоби захисту від витоку інформації в Інтернет.** Програмно-апаратні системи шифрування, брандмауери, системи попередження вторгнення.	8	2	2	4	7			7
Тема 9**. Протокол захисту електронних транзакцій TLS**. Порівняння версій протоколів TLS 2.0 та 3.0	8	2	2	4	7			7
Тема 10. **Захист електронної пошти.** Боротьба зі спамом та фішингом.	8	2	2	4	7			7
Тема 11. **Загрози інформаційної безпеки держави в соціальних мережах.**	8	2	2	4	7			7
Тема 12. **Безпека мережі з програмованими параметрами SDN.**	10	2	2	6	10			10
Тема 13. **Додаткові методи підвищення безпеки мережі ІКТ.**	8	2	2	4	13		2	11
Тема 14. **Створення та впровадження програми навчання працівників у сфері кібербезпеки** (SAT).	10	2	2	6	7			7
Усього годин	***120***	***28***	***28***	***64***	***120***	***6***	***6***	***108***
ПІДСУМКОВИЙ КОНТРОЛЬ – залік								

5. ТЕХНІЧНЕ Й ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ / ОБЛАДНАННЯ

Студенти отримують теми та питання курсу, основну і додаткову літературу, рекомендації, завдання та оцінки за їх виконання як традиційним шляхом, так і з використанням університетської платформи он-лайн навчання на базі Moodle (Google class). Окрім того, практичні навички під час виконання лабораторних робіт та виконання індивідуальних завдань, студенти отримують, користуючись університетськими комп'ютерними класами та бібліотекою. Технічні засоби навчання (мультимедійні та комп'ютерні пристрої). Програмне забезпечення: ОС (Linux), гіпервізори (VM VirtualBox), пакети та підсистеми шифрування даних (PGP, TrueCrypt, LUCKS/dm-crypt), утиліти-додатки для симуляції та виявлення загроз (Nmap, Honeyd).

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»	7	12
2	**Тема 2.** Вивчення Положення закону України «Про інноваційну діяльність»	7	12
3	**Тема 3.** Дослідження впливу витоку конфіденційної інформації на стан розвитку сучасного підприємсива.	8	12
4	**Тема 4.** Дослідження методів захисту від недоброчесної конкуренції та шпигунства**.**	8	12
5	**Тема 5.** Класифікація кіберзагроз та види кібератак.	8	12
6	**Тема 6.** Дослідження мережевих систем виявлення вторгнень.	8	12
7	**Тема 7.** Дослідження комплексного підходу виявлення вторгнень заснований на аналізі трафіка.	8	12
8	**Тема 8.** Дослідження порівняльної характеристики сучасних криптосистем, що використовуються для захисту конфіденційної інформації**.**	8	12
9	**Тема 9.** Дослідження протоколу захисту електронних транзакцій 3D-Secur для додаткового кроку автентифікації**.**	8	12
10	**Тема 10.** Класифікація загроз та правила поведінки працівників в корпоративній мережі.	8	12
11	**Тема 11.** Дослідження Віртуальних спільнот, як суб'єктів інформаційної безпеки Держави.	8	12
12	**Тема 12.** Дослідження моделі забезпечення безпеки в комп'ютерних системах.	8	12
13	**Тема 13.** Дослідження методів забезпечення якості обслуговування в комп'ютерних системах із самоподібними інформаційними потоками.	8	12
14	**Тема 14.** Дослідження програми навчання працівників у сфері кібербезпеки (SAT).	8	12
	Всього	***110***	***168***

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 заліку.	**50%**

Методи діагностики знань (контролю)	фронтальне опитування; наукова доповідь, тези доповіді, наукова стаття, індивідуальне опитування, тестування, залік.

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

Денна форма навчання			
Поточний контроль			
Види роботи	**Планові терміни виконання**	**Форми контролю та звітності**	**Максимальний відсоток оцінювання**
Систематичність і активність роботи на практичних заняттях			
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), що виноситься на самостійне вивчення	-//-	Розгляд відповідного матеріалу під час аудиторних занять або ІКР[1], перевірка конспектів навчальних текстів тощо	**10**
Виконання індивідуальних завдань (науково-дослідна робота студента)			
1.3. Підготовка індивідуального завдання згідно вказівок викладача	Відповідно до розкладу занять і графіку ІКР	Обговорення (захист) матеріалів індивідуального завдання	**10**
1.4. Інші види індивідуальних завдань, в т.ч. підготовка наукових публікацій, участь у роботі круглих столів, конференцій тощо.	-//-	Обговорення результатів проведеної роботи під час аудиторних занять або ІКР, наукових конференцій та круглих столів.	**5**
Разом балів за поточний контроль			**50**
Підсумковий контроль залік			**50**
Всього балів			**100**

Заочна форма навчання
Поточний контроль

[1] Індивідуально-консультативна робота викладача зі студентами

Види самостійної роботи	Планові терміни виконання	Форми контролю та звітності	Максимальний відсоток оцінювання
Систематичність і активність роботи під час аудиторних занять			
1.1. Підготовка до аудиторних занять	Відповідно до розкладу	Перевірка обсягу та якості засвоєного матеріалу під час аудиторних занять	**15**
За виконання контрольних робіт (завдань)			
1.2. Підготовка контрольних робіт (завдань) за заданою тематикою	-//-	Перевірка контрольних робіт, (завдань)	**15**
Виконання завдань для самостійного опрацювання			
1.3. Підготовка індивідуального завдання згідно вказівок викладача	-//-	Обговорення (захист) матеріалів індивідуального завдання	**10**
Виконання індивідуальних завдань (науково-дослідна робота студента)			
2.1. Підготовка індивідуального завдання за заданою тематикою, індивідуальних завдань, в т.ч. підготовка наукових публікацій, участь у роботі круглих столів, конференцій тощо	Відповідно до графіку ІКР	Обговорення (захист) матеріалів індивідуального завдання під час ІКР	**10**
Разом балів за поточний контроль			**50**
Підсумковий контроль залік			**50**
Всього балів підсумкової оцінки			**100**

9. КРИТЕРІЇ ПІДСУМКОВОЇ ОЦІНКИ ЗНАНЬ СТУДЕНТІВ
(для заліку)

Рівень знань оцінюється:

– «відмінно» / «зараховано» А – 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, практичних заняттях, під час яких виконував усі поставленні завдання та давав вичерпні, обґрунтовані, теоретично і практично правильні відповіді, виконав завдання до самостійної роботи, проявляє активність і творчість у науково-дослідній роботі;

– «добре» / «зараховано» В – 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, практичних заняттях, під час яких виконував усі поставленні завдання та давав вичерпні, обґрунтовані, теоретично і практично правильні відповіді, виконав завдання до самостійної роботи, проявляє активність і творчість у науково-дослідній роботі;

– «добре» / «зараховано» С – 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 виконаних індивідуальних завдань та завдань до самостійної роботи та активність у науково-дослідній роботі;

– «задовільно» / «зараховано» D - від 64 до 73 балів. Студент 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 виконаних індивідуальних завдань та завдань до самостійної роботи;

– «задовільно» / «зараховано» E – від 60 до 63 балів. Студент 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, виконав не всі завдання 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 1 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).

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

Допоміжна

1. ДСТУ 3396.1-96 Державний стандарт України Захист інформації. Технічний захист інформації. Порядок проведення робіт.
2. НД ТЗІ 1.1-002-99 Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу.
3. НД ТЗІ 1.1-003-99 Термінологія в галузі захисту інформації в комп’ютерних системах від несанкціонованого доступу.
4. НД ТЗІ 1.1-005-07 Захист інформації на об’єктах інформаційної діяльності. Створення комплексу ТЗІ. Основні положення.
5. НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу.
6. НД ТЗІ 3.3-001-07 Захист інформації на об’єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Порядок розроблення та впровадження заходів із захисту інформації.

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. 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.