КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ ТАРАСА ШЕВЧЕНКА

Факультет радіофізики, електроніки та комп'ютерних систем

Кафедра радіотехніки та радіоелектронних систем

«ЗАТВЕРДЖУЮ»

Заступник декана
з навчальної роботи
_____ О. Нечипорук
«__15__» _____ 2021 року

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

БЕЗПЕКА ІНФОРМАЦІЇ ТА КОНКУРЕНТНА РОЗВІДКА В ІНЖЕНЕРІЇ

для студентів

галузь знань	**17 Електроніка та телекомунікації**
спеціальність	**172 Телекомунікації та радіотехніка**
освітній рівень	**другий (магістр)**
освітня програма	**Інформаційна безпека телекомунікаційних систем і мереж**
вид дисципліни	**Обов'язковий компонент ОП**

Форма навчання	**денна**
Навчальний рік	**2021/2022**
Семестр	**1**
Кількість кредитів ECTS	**6**
Мова викладання, навчання та оцінювання	**українська**
Форма заключного контролю	**іспит**

Викладач:
Олександр Нікітчин,
канд. іст. наук, асистент кафедри радіотехніки та радіоелектронних систем

Пролонговано: на 20__/20__ н.р. _____ (_____) «___» _____ 20__ р.
на 20__/20__ н.р. _____ (_____) «___» _____ 20__ р

КИЇВ 2021

Розробник:

Олександр Нікітчин,
канд. іст. наук, асистент кафедри радіотехніки та радіоелектронних систем

ЗАТВЕРДЖЕНО

Завідувач кафедри радіотехніки та радіоелектронних систем
_____І. Анісімов

Протокол № 12 від "07" грудня 2021 р.

Схвалено науково-методичною комісією факультету радіофізики, електроніки та комп'ютерних систем

Протокол № 10 від "14" 12 2021 р.

Голова науково-методичної комісії _____С. Радченко

"____" _____ 2021 року

1. Мета дисципліни – є формування у студентів системи знань та умінь професійно організовувати роботу з інформаційно-аналітичного забезпечення безпеки підприємства, здійснювати управління та координування такою роботою, бути професіоналом у сфері конкурентної розвідки при організації та управлінні комплексним забезпеченням функціонування системи інженерно-технічної безпеки підприємств.

2. Попередні вимоги до опанування або вибору навчальної дисципліни:

Навчальна дисципліна "Безпека інформації та конкурентна розвідка в інженерії" є обов'язковою компонентою освітньої програми і є основою вивчення низки дисциплін вибору студента "ВБ х.01, ВБ х.02, ВБ х.03, ВБ х.04" відповідного вибіркового блоку цієї ОП, які, у свою чергу, є базою для обов'язкових компонент "Науково-виробнича практика" і "Дипломна робота магістра". Попередні вимоги:

1. Вміти запускати прикладні програмні засоби та керувати ними на основі графічного інтерфейсу користувача, орієнтуватись в файловій системі довільної ОС, знаходити інформацію в Інтернеті.
2. Знати основи алгоритмізації та вміти реалізувати багатофайловий проект консольного застосунку.
3. Знати принципи обміну даними у телекомунікаційних системах та реалізації розподілених систем.

3. Анотація навчальної дисципліни:

Дисципліна "Безпека інформації та конкурентна розвідка в інженерії" належить до переліку обов'язкових дисциплін ОП. Вона забезпечує професійний розвиток студента в галузі технічного захисту інформації та включає в себе розгляд принципів організації системи інформаційно-аналітичної діяльності, управління та проведення інженерних заходів по забезпеченню безпеки інформації та протидії конкурентній розвідці, що можуть бути використані при розробці, впровадженні та експлуатації апаратних засобів передачі, обробки та захисту інформації, при створенні автоматизованих систем управління, тощо. Вивчення цієї освітньої компоненти дозволить студенту вільно орієнтуватись в у сфері конкурентної розвідки при організації та управлінні комплексним забезпеченням функціонування системи інженерно-технічної безпеки підприємств.

4. Завдання (навчальні цілі):

1. Знати теоретичні основи інформаційно-аналітичного забезпечення безпеки підприємства.
2. Знати інформаційно-аналітичну роботу як засіб успішного розвитку сучасного підприємства.
3. Вміти організувати роботу інформаційно-аналітичного підрозділу підприємства.
4. Вміти використовувати досвід міжнародних компаній з організації інформаційно-аналітичного забезпечення безпеки підприємства.
5. Знати організацію конкурентної розвідки на підприємстві, її можливості у сфері стратегічного й тактичного управління бізнесом.
6. Вміти застосовувати інформаційно-аналітичну роботу як засіб попередження промислового шпигунства та протидії загрозам безпеки бізнесу.

Забезпечити досягнення компетентностей:

ЗК 2. Здатність застосовувати знання у практичних ситуаціях.
ЗК 3. Знання та розуміння предметної області та розуміння професійної діяльності.
ЗК 4. Навички використання інформаційних і комунікаційних технологій.
ФК 2. Здатність забезпечувати інформаційну безпеку під час виконання дослідження для потреб розробки телекомунікаційних та радіотехнічних виробів і систем.
ФК 4. Здатність виконувати монтаж, налагодження, експлуатацію, контроль технічного стану технологічного та лабораторного телекомунікаційного та радіотехнічного обладнання.

5. Результати навчання за дисципліною:

Результат навчання (1 знати; 2 вміти; 3 комунікація; 4 автономність та відповідальність)		Форми (та/або методи і технології) викладання і навчання	Методи оцінювання та пороговий критерій оцінювання (за необхідності)	Відсоток у підсумковій оцінці з дисципліни
Код	Результат навчання			
1	студент повинен **знати:**	лекційні заняття, семінарські заняття, лаб. роботи	виконання самостійних та лабораторних робіт, усні доповіді на семінарських заняттях	до 40
1.1	методологію інформаційно-аналітичної діяльності	- // - // - // -	- // - // - // -	10
1.2	способи збору інформації її класифікації та перевірки	- // - // - // -	- // - // - // -	10
1.3	особливості організації конкурентної розвідки на підприємстві	- // - // - // -	- // - // - // -	10
1.4	можливості новітніх технологій для оптимізації роботи інформаційно-аналітичного підрозділу	- // - // - // -	- // - // - // -	10
2	студент повинен **вміти**:	лекційні заняття, семінарські заняття, лаб. роботи	виконання самостійних та лабораторних робіт, усні доповіді на семінарських заняттях	до 40
2.1	професійно організувати роботу з інформаційно-аналітичного забезпечення безпеки підприємства	- // - // - // -	- // - // - // -	10
2.2	використовувати методи протидії конкурентній розвідці для збору інформації	- // - // - // -	- // - // - // -	10
2.3	формувати аналітичну стратегію безпеки підприємства	- // - // - // -	- // - // - // -	10
2.4.	користуючись електричними схемами класифікувати радіоелектронні пристрої, побудовані на базі напівпровідникових приладів, пояснити їхнє призначення та принципи функціонування	- // - // - // -	- // - // - // -	10
3	**комунікація**	лекційні заняття, семінарські заняття, лаб. роботи	виконання самостійних та лабораторних робіт, усні доповіді на семінарських заняттях	до 10
3.1	вміти професійно організувати роботу з інформаційно-аналітичного забезпечення безпеки підприємства; здійснювати управління роботою інформаційно-аналітичного підрозділу; використовувати методи	- // - // - // -	- // - // - // -	10

	протидії конкурентній розвідці для збору інформації; формувати аналітичну стратегію безпеки підприємства; аналізувати, обробляти отриману інформацію та подавати висновки;			
4	**автономність та відповідальність**	лекційні заняття, семінарські заняття, лаб. роботи	виконання самостійних та лабораторних робіт, усні доповіді на семінарських заняттях	до 10
4.1	розуміти особливості організації конкурентної розвідки на підприємстві; напрямки діяльності підрозділу конкурентної розвідки; можливості новітніх технологій для оптимізації роботи конкурентної розвідки; організацію роботи конкурентної розвідки відомих міжнародних компаніях;	- // - // - // -	- // - // - // -	10

6. Співвідношення результатів навчання дисципліни із програмними результатами навчання

Результати навчання дисципліни (код) / **Програмні результати навчання (назва)**	1.1	1.2	1.3	1.4	2.1	2.2	2.3	2.4	2.5	2.6	3.1	4.1
ПРН 3. Знати аналогову та цифрову схемотехніку, методи та засоби їх моделювання та конструювання, використання для досліджень.	+			+								
ПРН 4. Знати аналогові та цифрові, в тому числі адаптивні, методи обробки інформації.		+		+								
ПРН 5. Знати архітектуру телекомунікаційних систем, їх апаратні та програмні складові, їх теоретичне обгрунтування.			+									
ПРН 6. Знати сучасні телекомунікаційні та мережеві технології, тенденції їх розвитку.				+								
ПРН 7. Знати теоретичні основи та принципи забезпечення інформаційної безпеки.					+							
ПРН 9. Знаходити і аналізувати потрібну для роботи наукову та інженерно-технічну інформацію.					+	+						

7. Схема формування оцінки

7.1. Форми оцінювання студентів: рівень досягнення всіх запланованих результатів навчання визначається за результатами поточного контролю за процесом виконання самостійних робіт та

оцінювання кінцевих результатів їх виконання і за результатами виконання самостійних завдань. Вклад результатів навчання у підсумкову оцінку, за умови їх опанування на належному рівні:

- результати навчання 1.1 – 1.6 [**знання**] до 40 %;
- результат навчання 2.1 – 2.3 [**вміння**] – до 40%;
- результат навчання 3.1 [**комунікація**] – до 10%;
- результат навчання 4.1 [**автономність та відповідальність**] – до 10%.

Форми оцінювання студентів:

- **семестрове оцінювання**: контроль здійснюється за таким принципом. Навчальний семестр має два змістові модулі: у змістовий модуль 1 (ЗМ1) входять теми 1-4, у змістовий модуль 2 (ЗМ2) входять теми 5-7. Оскільки виконання самостійних робіт повністю охоплює перевірку засвоєння лекційного матеріалу, контрольні роботи не проводяться. Загальне оцінювання протягом семестру виконується за сумою результатів виконання самостійних робіт. Обов'язковим для допуску до іспиту є виконання самостійних робіт кожного з модулів з сумарною оцінкою не менше 18 балів (з 30) за кожну. Оцінка за виконання студентами самостійних завдань дозволяє компенсувати недобір балів за модуль, надлишкові бали (більше 30 за модуль) відкидаються.
- **підсумкове оцінювання (у формі іспиту):** форма іспиту – письмова робота (оцінюється від 0 до 40 балів). Умовою досягнення позитивної оцінки за дисципліну є отримання загальної суми балів (за семестрове оцінювання та іспит разом) не менш ніж 60 балів, при цьому оцінка за фінальне оцінювання не може бути меншою 24 балів.
- **умови допуску до підсумкового оцінювання:** умовою допуску до іспиту є отримання студентом сумарно не менше, аніж *критично-розрахунковий мінімум 36 балів* за семестр.

7.2. Організація оцінювання:

Оцінювання за формами контролю:

	ЗМ1		***ЗМ2***	
	Мін. – балів	*Мах. – балів*	*Мін. – балів*	*Мах. – балів*
Модуль 1	18	30		
Модуль 2			18	30
Виконання самостійних завдань	0	5	0	5

Орієнтовний графік оцінювання:

	Орієнтовний період для здійснення відповідної форма оцінювання
Виконання завдань самостійної роботи	вересень-грудень
Іспит	грудень

Розрахунок балів, які студент отримує при успішній здачі іспиту:

	Змістовий модуль 1	Змістовий модуль 2	Іспит	Підсумкова оцінка
Мінімум	*18*	*18*	*24*	*60*
Максимум	**30**	**30**	**40**	**100**

7.3. Шкала відповідності оцінок

Оцінка (за національною шкалою) / National grade	Рівень досягнень, % / Marks, %
Відмінно / Excellent	90-100%
Добре / Good	75-89%
Задовільно / Satisfactory	60-74%
Незадовільно / Fail	0-59%

8. Структура навчальної дисципліни. Тематичний план занять.

№ з/п	Назва теми	Кількість годин			
		лекції	лаб. роботи	семінари	самост. робота
Змістовий модуль 1. Конкурента розвідка – пріоритетний напрямок розвитку бізнесу					
1	Вступ. Поняття та особливості конкурентної розвідки. Історія становлення та розвитку конкурентної розвідки.	4		2	10
2	Завдання та особливості конкурентної розвідки. Бенчмаркінг як складова успішної бізнес-стратегії	6	2	2	10
3	Фактори впливу на безпеку бізнесу. Формування системи інформаційної безпеки бізнесу.	6		2	20
4	Вплив інформаційних війн на безпеку бізнесу та механізм протидії інформаційній зброї.	6	2	2	20
Змістовий модуль 2. Організація конкурентної розвідки на підприємстві, її можливості у сфері стратегічного й тактичного управління бізнесом					
5	Організація роботи підрозділу конкурентної розвідки. Передумови та порядок створення конкурентної розвідки на підприємстві. Напрямки діяльності конкурентної розвідки. Стратегія та шляхи визначення інформаційних потреб керівництва компанії у діяльності конкурентної розвідки.	6		2	20
6	Методи конкурентної розвідки. Методика конкурентної розвідки. Протидія промисловому шпигунству. Класифікація методів конкурентної розвідки. Поняття, характерні особливості та ознаки дезінформації.	6	2	2	20
7	Загальна характеристика організації конкурентної розвідки у європейських та американських компаніях	6		2	20
	Всього	40	6	14	120

Загальний обсяг **180** год., з них:
лекцій – **40** год.;
лабораторних робіт – **6** год.;
семінарських занять – **14** год.;
самостійна робота – **120** год.

9. Рекомендовані джерела

Основні:

1. Miller J. Millenium Intelligence; Understanding and Conducting Competative Intelligence in the Digital Age, Business Intelligence Braintrust, 2000.- 469 p.
2. Ховис Д. Конкурентна розвідка. Уроки з окопов / Д. Ховис : "Альпина Паблишер ", 2003. – 532 с.
3. Міщишин М. Конкурентна розвідка – об'єктивна необхідність у сучасному бізнесі / М. Міщишин // Контракти. – 2006. – № 7. – С. 38
4. Качинський А.Б. Безпека, загрози і ризик: наукові концепції та математичні методи / А.Б. Качинський; Інститут проблем національної безпеки; Національна академія Служби безпеки України. - К., 2004. - 472с.
5. Рафалевський О. Служба безпеки підприємства під ключ.- Електронний ресурс. – Режим доступу до статті: www.security_info.com.ua
6. Шейко В.М., Кушнаренко Н.М. Організація та методика науково-дослідницької діяльності: підручник. – 6-те видання / В.М. Шейко, Н.М. Кушнаренко. – К. : Знання, 2008. – 310 с.

Додаткові:

7. Артемчук Г.І., Кирило В.М., Кочерган М.П. Методика організації науково-дослідної роботи / Г.І. Артемчук, В.К. Кирило, М.П. Кочерган : Навч. посібник. – К. : Форум, 2000. – 271 с.
8. Іваницька Н. Промислове шпигунство та правові інструменти захисту від нього / Н. Іваницька // Бизнес и безопасность. - № 1. – 2006. – С. 21-28
9. Griffin, Robert J. Just Do It: Establishing a Corporate Business Intelligence Function at IBM, Proceedings, SCIP 12th Annual International Conference and Exhibits. – Vol. II. – 2004. – P. 123-133.
10. Herring, Jan P. Business Intelligence in Japan and Sweden: Lessons for the US, The Journal of Business Strategy. – March/ April 2002. – P. 21-44
11. Новикова О.Ф. Економічна безпека: концептуальне визначення та механізм забезпечення. /О.Ф.Новікова, Р.В.Покотоленко; [наук. ред. О.І.Амоша]; НАН України, Ін-т економіки пром-сті. – Донецьк.:,2006. - 407 с.
12. Miller J. Millenium Intelligence; Understanding and Conducting Competative Intelligence in the Digital Age, Business Intelligence / J. Miller. – Braintrust, 2000. – 312 с.