



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

СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Спеціальні вимірювання в галузі ТЗІ

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
Доцент кафедри Комп'ютерної інженерії та інноваційних технологій Онацький Олексій Віталійович	+380503761048	onatsky@meta.ua

1. АНОТАЦІЯ ДО КУРСУ

Спеціальні вимірювання в галузі ТЗІ 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 розглядається порядок проведення робіт з технічного захисту інформації, а саме: заходи з технічного захисту мовної інформації; заходи з технічного захисту інформації, яка обробляється в інформаційно-комунікаційних системах; сутність, шляхи та запобігання утворення технічних каналів витоку інформації: мовної та візуальної інформації, матеріально-речовинні канали витоку інформації, технічні канали витоку інформації, що обробляється основними та допоміжними технічними засобами системи, технічні канали витоку інформації на основі закладних пристроїв.

Метою викладання навчальної дисципліни Спеціальні вимірювання в галузі ТЗІ є забезпечення здобувачів знаннями з методів впровадження систем та комплексів захисту інформації, їх склад і призначення, з застосуванням існуючої нормативної бази в

Україні; розвиток у студентів практичних навичок у послідовності розробки комплексу технічного захисту інформації; підготовка висококваліфікованих фахівців, здатних ставити завдання на виконання етапів технічного проекту і вибирати способи їх реалізації.

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

ІК1. 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.

КЗ4. Здатність оцінювати та забезпечувати якість виконуваних робіт.

Спеціальні (фахові, предметні) 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.

КФ2. Здатність розробляти, впроваджувати та аналізувати нормативні документи, положення, інструкції й вимоги технічного та організаційного спрямування, а також інтегрувати, аналізувати і використовувати кращі світові практики, стандарти у професійній діяльності в сфері інформаційної безпеки та/або кібербезпеки.

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

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

РН5. Критично осмислювати проблеми інформаційної безпеки та/або кібербезпеки, у тому числі на міжгалузевому та міждисциплінарному рівні, зокрема на основі розуміння нових результатів інженерних і фізико-математичних наук, а також розвитку технологій створення та використання спеціалізованого програмного забезпечення.

РН6. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення.

РН7. Обґрунтовувати використання, впроваджувати та аналізувати кращі світові стандарти, практики з метою розв'язання складних задач професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.

PH13. 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.

PH23. Обґрунтовувати вибір програмного забезпечення, устаткування та інструментів, інженерних технологій і процесів, а також обмежень щодо них в галузі інформаційної безпеки та/або кібербезпеки на основі сучасних знань у суміжних галузях, наукової, технічної та довідкової літератури та іншої доступної інформації.

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	28 /	28 /	64 /	1	2 /	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
Змістовий модуль 1. Спеціальні вимірювання в галузі ТЗІ.							
Тема 1. Базові принципи, поняття та терміни у сфері ТЗІ.	18	4	4	10			
Тема 2. Сучасні підходи до формування вимог до захисту інформації	9	2	2	5			
Тема 3. Поняття КСЗІ та КТЗІ, їх склад і призначення.	9	2	2	5			

Тема 4. Класифікація технічних каналів витоку інформації.	18	4	4	10				
Тема 5. Порядок проведення робіт з технічного захисту інформації.	9	2	2	5				
Тема 6. Створення комплексів технічного захисту інформації.	9	2	2	5				
Тема 7. Форми та зміст моделей загроз та порушника для інформації	9	2	2	5				
Тема 8. Порядок розробки та зміст технічних проектів КСЗІ та КТЗІ.	9	2	2	5				
Тема 9. Попередні випробування та дослідна експлуатація КТЗІ.	8	2	2	4				
Тема 10. Атестації комплексів технічного захисту інформації.	8	2	2	4				
Тема 11. Система технічних документів щодо систем і КЗІ.	8	2	2	4				
Тема 12. Порядок проведення робіт з державної експертизи КСЗІ.	8	2	2	4				
Усього годин	120	28	28	64				
ПІДСУМКОВИЙ КОНТРОЛЬ – Екзамен								

5. ТЕХНІЧНЕ Й ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ / ОБЛАДНАННЯ

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

6. САМОСТІЙНА РОБОТА

До самостійної роботи студентів щодо вивчення дисципліни «Спеціальні вимірювання в галузі ТЗІ» 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. Базові принципи, поняття та терміни у сфері ТЗІ. Закони, нормативні акти, нормативні документи, що визначають вимоги із захисту інформації та кіберзахисту.	10	

2	Тема 2. Сучасні підходи до формування вимог до захисту інформації. Сутність, шляхи та запобігання утворення технічних каналів витоку інформації.	5	
3	Тема 3. Поняття КСЗІ та КТЗІ, їх склад і призначення. Розробка політики безпеки інформаційно-комунікаційних системах.	5	
4	Тема 4. Класифікація технічних каналів витоку інформації. Обстеження середовищ функціонування ІТС.	5	
5	Тема 5. Порядок проведення робіт з технічного захисту інформації. Формування вимог до КСЗІ та її завдань. Категоріювання ІТС.	8	
6	Тема 6. Створення комплексів технічного захисту інформації. Розробка моделі загроз на об'єкті інформаційної діяльності.	5	
7	Тема 7. Форми та зміст моделей загроз та порушника для інформації. Розробка моделі порушника інформації. Розробка моделі загроз для інформації.	5	
8	Тема 8. Порядок розробки та зміст технічних проектів КСЗІ та КТЗІ. Розробка ТЗ на створення КСЗІ та КТЗІ.	5	
9	Тема 9. Попередні випробування та дослідна експлуатація КТЗІ. Розробка програми та методики проведення атестації комплексів технічного захисту інформації	4	
10	Тема 10. Атестації комплексів технічного захисту інформації. Протокол інструментального контролю захищеності інформації на об'єкті інформаційної діяльності.	4	
11	Тема 11. Система технічних документів щодо систем і КЗІ. Оформлення документації.	4	
12	Тема 12. Порядок проведення робіт з державної експертизи КСЗІ. Супровід КСЗІ.	4	
	Всього	64	

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			
<i>Поточний контроль</i>			
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
<i>Підсумковий контроль – екзамен</i>			50
Всього балів			100

Заочна форма навчання

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

Рівень знань оцінюється:

- «відмінно» / «зараховано» А - 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» В - 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» С - 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	Не зараховано
60-63 (4)	E		
35-59 (3)	FX	Незадовільно	
1-34 (2)	F		

10. РЕКОМЕНДОВАНА ЛІТЕРАТУРА

Основна

1. НД ТЗІ 3.7-003-05. Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі. – Затверджено наказом ДСТСЗІ СБ України № 125 від 8.11.2005. – (Серія видань “Нормативний документ”).

2. Положення про Державну експертизу в сфері технічного захисту інформації. – Затверджено наказом Адміністрації ДССЗЗІ України № 93 від 16.05.07. – Офіційний вісник України. – 2007. – № 52, ст. 2153. – (Серія видань “Нормативний документ”).

3. НД ТЗІ 2.6-001-11. Порядок проведення робіт з державної експертизи засобів технічного захисту інформації від несанкціонованого доступу та комплексних систем захисту інформації в інформаційно-телекомунікаційних системах. – Затверджено наказом Адміністрації ДССЗЗІ України № 65 від 12 березня 2011. – (Серія видань “Нормативний документ”).

4. Богуш В.М., Кривуца В.Г., Кудін А.М. Інформаційна безпека: Термінологічний навчальний довідник / За ред. Кривуци В.Р – Київ.: ООО "Д.В.К.", 2004. – 508 с.

5. Засоби та системи технічного захисту інформації : навч. посіб. для студентів спеціальності 125 "Кібербезпека" спеціалізації "Системи технічного захисту інформації" / І. Є. Антіпов, А. М. Олейніков, Ю. В. Ликов и др. ; М-во освіти і науки України, Харків. нац. ун-т радіоелектроніки. – Харків : ХНУРЕ, 2019. – 216 с.

6. Домарев В.В., Скворцов С.О. Організація захисту інформації на об'єктах державної та підприємницької діяльності. Навчальний посібник. – К.: Вид-во Європ. Ун-ту, 2006. – 102 с.

Допоміжна

1. ДСТУ 33960-96 Захист інформації. Технічний захист інформації. Основні положення.

2. ДСТУ 3396.1-96. Захист інформації. Технічний захист інформації. Порядок проведення робіт.

3. НД ТЗІ 1.6-005-2013. Захист інформації на об'єктах інформаційної діяльності. Положення про категоріювання об'єктів, де циркулює інформація з обмеженим доступом, що не становить державної таємниці

4. НД ТЗІ 1.4-001-2000. Типове положення про службу захисту інформації в автоматизованій системі.

5. Про внесення змін до Закону України “Про захист інформації в автоматизованих системах ” № 2594-IV від 31.05.2005. – Відомості Верховної Ради України 2005, № 26, ст. 347. – (Серія видань “Законодавство України”).

6. Богуш В.М., Кривуца В.Г., Кудін А.М. Інформаційна безпека: Термінологічний навчальний довідник / За ред. Кривуци В.Р – Київ.: ООО "Д.В.К.", 2004. – 508 с.

Інформаційні ресурси

1. Сайт Державної служби спеціального зв'язку та захисту інформації. URL: <https://cip.gov.ua/ua>.

2. Сайт Технічний захист інформації. URL:<https://tzi.ua/ua/index.html>.

3. Комплексні системи захисту інформації. URL:

https://web.posibnyky.vntu.edu.ua/fmib/41yaremchuk_kompleksni_systemy_zahystu_informaciyi/

4. Комплексні системи захисту інформації. Проектування, впровадження, супровід. URL:

https://books.google.com.ua/books?id=GcBIDwAAQBAJ&printsec=frontcover&hl=ru&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false

5. Сайт Computer Emergency Response Team of Ukraine. URL: <https://cert.gov.ua>.

6. <https://zakon.rada.gov.ua/laws>.