Національний технічний університет України
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»

Інститут спеціального зв'язку та захисту
інформації КПІ ім. Ігоря Сікорського
Спеціальна кафедра № 1

ТЕХНІЧНИЙ ЗАХИСТ ІНФОРМАЦІЇ

Робоча програма навчальної дисципліни (силабус)

Рівень вищої освіти	***Перший (бакалаврський)***
Галузь знань	*12 Інформаційні технології*
Спеціальність	*122 Комп'ютерні науки,*
Освітньо-професійна програма	*Комп'ютерні системи і технології спеціального зв'язку*
Статус дисципліни	*Вибіркова*
Форма навчання	*очна (денна)*
Рік підготовки, семестр	*III рік підготовки, осінній семестр*
Обсяг дисципліни	*5 кредитів ECTS/150 годин (18 годин лекцій, 28 годин практичних занять, 26 годин лабораторних робіт)*
Семестровий контроль/ контрольні заходи	*залік*
Мова викладання	*Українська*
Інформація про керівника курсу / викладачів	Лектор: Сергій Іванченко Практичні заняття: Сергій Іванченко Лабораторні роботи: Сергій Іванченко
Розміщення курсу	Google Classroom

Київ – 2022

Програма навчальної дисципліни

1. Опис навчальної дисципліни, її мета, предмет вивчання та результати навчання

Силабус освітнього компонента “Технічний захист інформації” складено відповідно до освітньої програми підготовки бакалаврів “Комп’ютерні системи і технології спеціального зв’язку” спеціальності 122 Комп’ютерні науки.

Метою навчальної дисципліни є підсилення та закріплення у здобувачів вищої освіти наступних компетентностей: (ЗК 1) Здатність до абстрактного мислення, аналізу та синтезу; (ЗК 2) Здатність застосовувати знання у практичних ситуаціях; (ЗК 6) Здатність вчитися й оволодівати сучасними знаннями; (СК 7) Здатність застосовувати теоретичні та практичні основи методології та технології моделювання для дослідження характеристик і поведінки складних об'єктів і систем, проводити обчислювальні експерименти з обробкою й аналізом результатів;

Предметом навчальної дисципліни є методи організації технічного захисту інформації.

Програмні результати навчання, на підсилення та покращення яких спрямована дисципліна: (ПР 1) Застосовувати знання основних форм і законів абстрактно-логічного мислення, основ методології наукового пізнання, форм і методів вилучення, аналізу, обробки та синтезу інформації в предметній області комп'ютерних наук; (ПР 2) Використовувати сучасний математичний апарат неперервного та дискретного аналізу, лінійної алгебри, аналітичної геометрії, в професійній діяльності для розв’язання задач теоретичного та прикладного характеру в процесі проектування та реалізації об’єктів інформатизації; (ПР 22) Зберігати та примножувати досягнення і цінності суспільства на основі розуміння місця предметної області у загальній системі знань, використовувати різні види та форми рухової активності для ведення здорового способу життя.

2. Пререквізити та постреквізити навчальної дисципліни (місце в структурно-логічній схемі навчання за відповідною освітньою програмою)

Для успішного засвоєння дисципліни здобувач вищої освіти повинен володіти освітніми компонентами “Цифрова обробка сигналів”, “Фізика”, “Основи теорії інформації кодування”. Компетенції, знання та уміння, одержані в процесі вивчення освітнього компонента є необхідними для подальшого вивчення освітніх компонентів “Основи протидії технічним розвідкам”, “Військове стажування”.

3. Зміст навчальної дисципліни

Семестр 5

Семестровий (кредитний) модуль 1. Технічний захист інформації.
Розділ 1. Технічний захист інформації.
Тема 1. Інформація як об’єкт захисту та технічний захист інформації.
Основні визначення та положення.

Тема 2. Технічні канали витоку інформації, їх різновиди сутність.
Основні поняття з витоку інформації.

Класифікація технічних каналів витоку інформації: технічні канали витоку інформації, що утворюються від основних технічних засобів і систем, електромагнітні канали витоку інформації, технічні канали витоку інформації через допоміжні технічні засоби та системи і сторонні провідники, електричні канали витоку інформації, параметричні канали витоку інформації, що обробляються в основних технічних засобах та системах.

Технічні канали витоку мовної інформації: акустичні канали витоку інформації, акустично-вібраційні канали витоку інформації, акустично-електричні канали витоку

інформації, акустично-оптичні канали витоку інформації, параметричні канали витоку мовної інформації.

Виток інформації через засоби прихованого добування інформації: сутність та класифікація засобів несанкціонованого перехоплення інформації, загальні характеристики засобів та сутність типових закладних пристроїв (радіозакладні пристрої. Закладні пристрої типу «довге вухо», закладні пристрої з надлишковим випромінюванням, мережеві закладні пристрої), напрямки захисту від закладних пристроїв.

Практика. Виток інформації в каналах зв'язку, виток видової інформації та матеріально-речовинні канали витоку: виток інформації в каналах зв'язку, виток видової інформації, матеріально-речовинні канали витоку інформації. Способи добування інформації з магнітних носіїв.

Тема 3. Базові регламентуючі положення в сфері технічного захисту інформації в Україні.

Основні положення в сфері технічного захисту інформації в Україні. Положення про технічний захист інформації в Україні. Контроль за функціонуванням Положення про технічний захист інформації в Україні. Положення про державну експертизу в сфері технічного захисту інформації.

Положення про службу захисту інформації. Створення комплексів технічного захисту інформації на об'єктах інформаційної діяльності. Захист інформації на об'єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Передпроектні роботи НД ТЗІ 3.1-001-07.

Проведення перед проектних досліджень на об'єкті інформаційної діяльності. Основні положення перед проектних досліджень на об'єкті інформаційної діяльності. Основні етапи проведення перед проектних досліджень. Розроблення технічного завдання на виконання робіт із створення комплексу захисту на об'єкті інформаційної діяльності.

Порядок розроблення технічного завдання. Вимоги до змісту розділів технічного завдання. Перехоплення даних. Класифікація каналів витоку інформації. Технічні канали витоку інформації. Основні причини виникнення електричних каналів витоку інформації. Порушники інформаційної безпеки та їх класифікація. Перехоплення даних та канали витоку інформації. Моніторинг радіотехнічних каналів. Доглядові портативні телевізійні системи.

Практика. Програмно-апаратні засоби моніторингу радіотехнічних каналів. Піранья ST-031, радіолокатор NR-900, Tektronix RSA 306. Панорамні приймачі та нелінійні радіолокатори NR-900. Виявлення та блокування засобів негласного отримання інформації на об'єктах інформаційної діяльності. Методика виявлення джерел акустичної або відеоінформації. (VEGA 09., Піранья ST 031, Flir i5) Проведення комплексу організаційних і технічних заходів з обстеження приміщень з метою виявлення технічних каналів витоку інформації.

Тема 4. Методи та засоби захисту технічних каналів від витоку інформації на об'єктах інформаційної діяльності.

Класифікація технічних каналів витоку інформації. Перехоплення даних. Захист інформації від витоку технічними каналами. Принципи блокування технічних каналів витоку інформації. Захист інформації від витоку через закладні пристрої. Поняття інженерно-технічного захисту. Фізичні засоби захисту: охоронні системи, охоронне телебачення, охоронне освітлення та засоби охоронної сигналізації. Поняття інженерно-технічного захисту.

Охоронне телебачення, охоронне освітлення та засоби охоронної сигналізації. Захист елементів будинків і приміщень. Апаратні засоби захисту. Ключові елементи, персональні кодові карти, персональний ідентифікатор, пристрої розпізнавання голосу користувача чи форми його пальців. Апаратні засоби захисту інформації. Основи апаратного захисту. Комплексні спеціальні перевірки, пошукові заходи та засоби.

Основні завдання комплексних спеціальних перевірок. Класифікація закладних пристроїв та їх демаскуючі ознаки. Технічні засоби пошуку засобів негласного знімання інформації. Закладні пристрої, їх основні характеристики та застосування. Способи та засоби боротьби. Класифікація закладних пристроїв. Основні характеристики закладних пристроїв. Структура радіоканалів витоку інформації .

Практика. Закладні пристрої, їх основні характеристики та застосування. Способи та засоби боротьби. Класифікація радіоканалів витоку інформації. Класифікація акустичних каналів. Класифікація пристроїв несанкціонованого зняття інформації. Способи та засоби боротьби з закладними пристроями. Побічні електромагнітні випромінювання та наведення. Методи виявлення пристроїв несанкціонованого зняття інформації

Тема 5. Технічний захист інформації на мережевому рівні.

Технічний захист інформації на мережевому рівні. Міжмережеві екрани. Технічний захист інформації від несанкціонованого доступу на апаратному рівні. Система виявлення вторгнень. Системи технічного захисту інформації в Україні: стан, проблемні питання та напрями розвитку. Проблеми захисту інформації в Україні.

Правові та нормативно-методичні проблеми. Проблеми метрології та регламенту в системі ТЗІ. Засоби технічного захисту інформації на ринку України та дозвіл користування ними. Класифікатор засобів технічного захисту інформації НД ТЗІ 1.5-002-2012. Основні положення, терміни та визначення.

Перелік та класифікація основних засобів технічного захисту інформації. Зміст і послідовність робіт з підготовки та проведення комплексних спеціальних перевірок приміщень. Мета проведення спеціальної комплексної перевірки приміщень. Етапи виконання перевірки.

Практика. Пошук закладних пристроїв з радіочастотним каналом передачі на основі радіомоніторингу.

Локалізація місця розташування радіовипромінювальних закладних пристроїв за допомогою пошукового приладу ST 031 «Піранья».

Підготовка контрольованого приміщення. Методи пошуку: амплітудний метод пошуку, метод пошуку «акустичної зав'язки». Перевірка телефонних ліній. Пошук закладних пристроїв, що використовують провідні комунікації. Пошук закладних пристроїв, що використовують низькочастотні магнітні випромінювання. Пошук сигналів і локалізація джерел.

4. Навчальні матеріали та ресурси

4.1. Основна література

1. Технічні канали витоку інформації. Порядок створення комплексів технічного захисту інформації. Навчальний посібник / Іванченко С.О., Гавриленко О.В., Липський О.А., Шевцов А.С. – К.: ІСЗЗІ НТУУ «КПІ», 2015. – 104 с.

2. Методи та засоби інженерно-технічного захисту інформації навч. посіб. / В.В. Богданов, О.В.Волков, О.В.Жук, В.В.Мартинюк – К.: ВІТІ НТУУ «КПІ», 2013.

3. Захист інформації обмеженого доступу: навч. посіб. / Г.А. Бузов – М.: Гаряча лінія - Телеком, 2014.

4. «Про захист інформації в інформаційно-телекомунікаційних системах» Закон України від 05.07.1994 № 80/94-ВР (В редакції Закону від 31.05.2005 № 2594-IУ).

5. Конституція України: редакція від 01.01.2020 р./ Відомості Верховної Ради України, № 254к/96-ВР, ст.141

6. «Про основи національної безпеки України» Закон України від 19.06.2003р.. № 964-IV, ВВР, 2003, №39, ст.351 (редакція станом на 08.07.2018),.

7. «Про інформацію» Закон України від 02.10.1992 р., №2657-XII, ВВР, 1992, №48, ст.650 (редакція станом на 16.07.2020).

8. «Про державну таємницю» Закон України від 21.01.1994 р., № 3855-XII, ВВР, 1994, № 16, ст.93 (редакція станом на 24.10.2020).

9. «Про власність» Закон України в редакції від 20.06.2007 р. № 697-XII, ВВР, 2007, №33, ст. 440.

10. ДСТУ 3396.0-96. Захист інформації. Технічний захист інформації. [Чинний від 1997-01-01]. Київ, Держстандарт України, 1997, ст. 20.

11. ДСТУ 3396.1-96. Захист інформації. Технічний захист інформації. Порядок проведення робіт. [Чинний від 1997-07-01]. Київ Держстандарт, 1997, ст. 6.

12. ДСТУ 3396.2-97. Захист інформації. Технічний захист інформації. Терміни та визначення. [Чинний від 1998-01-01]. Київ, Держстандарт України, 1997, ст. 12.

13. ДБН А.2.2-2-96 Проектування. Технічний захист інформації. Загальні вимоги до організації проектування та проектної документації для будівництва. [чинний від 1997-01-01, в редакції від 2005-08-23]. Київ. Держстандарт. 2005, ст. 13.

14. ДСТУ 3396 0-96 Захист інформації. Технічний захист інформації. Основні положення. [Чинний від 1997-01-01]. Київ, Держстандарт України, 1997, ст. 20.

15. ДСТУ 3396 1-96 Захист інформації. Технічний захист інформації. Порядок проведення робіт. [Чинний від 1997-07-01]. Київ Держстандарт, 1997, ст. 6.

16. ДСТУ 3396.2-97 Захист інформації. Технічний захист інформації. Терміни та визначення. [Чинний від 1998-01-01]. Київ, Держстандарт України, 1997, ст. 12.

17. Захист інформації обмеженого доступу: навч. посіб. / Г.А. Бузов – М.: Гаряча лінія - Телеком, 2014.

18. Звід відомостей, що становлять державну таємницю (затверджено наказом служби безпеки України від 12.08.2005 № 440, із змінами).

19. Наказ Адміністрації Держспецзв'язку від16.05.2007 № 93, зареєстрований в Міністерстві юстиції України 16.07.2007 за №820/14087 із змінами, затвердженими наказом Адміністрації Держспецзв'язку від 10.10.2012 №567, зареєстрованим в Міністерстві юстиції України 06.11.2012 за № 1863/22175. «Положення про державну експертизу в сфері технічного захисту інформації».

20. Наказ Адміністрації Держспецзв'язку від 04.07.2008 № 112, зареєстрований в Міністерстві юстиції України 25.07.2008 за № 690/15381 «Про затвердження Порядку оцінки стану захищеності державних інформаційних ресурсів в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах».

21. НД ТЗІ 1.1-002-1999 Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу. [в редакції станом на 28.12.2012. Київ. ДСТСЗІ СБ України, 2012, ст. 21.

22. НД ТЗІ 3.6-003-2016 Порядок проведення робіт зі створення та атестації комплексу технічного захисту інформації.

23. Постанова Кабінету Міністрів України від 16.02.1998 № 180 «Про затвердження Положення про забезпечення режиму секретності під час обробки інформації, що становить державну таємницю, в автоматизованих системах».

24. Постанова Кабінету Міністрів від 29.03.2006 № 373 «Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах».

25. Технічні канали витоку інформації: навч. посіб. / Ю.Б. Науменко, Н.А. Паламарчук, С.А. Паламарчук, О.Є. Ткаленко – К.: ВІТІ НТУУ «КПІ», 2010.

26. Технічно-експлуатаційна документація до відповідних технічних засобів, систем та комплексів технічного захисту інформації, що вивчаються.

27. Тимчасові рекомендації з технічного захисту інформації у засобах обчислювальної техніки, автоматизованих системах і мережах від витоку каналами побічних електромагнітних випромінювань і наводок (ТР ЕОТ-95).

28. Тимчасові рекомендації з технічного захисту інформації від витоку каналами побічних електромагнітних випромінювань і наводок. (ТР ТЗІ – ПЕМВН-95).

4.2. Додаткова література

1. ДСТУ 4163-03 Державна уніфікована система документації. Уніфікована система організаційно-розпорядчої документації. Вимоги до оформлювання документів. [Чинний від 2003-09-01]. Київ, Держстандарт, 2003, ст. 40.

2. Постанова Кабінету Міністрів України від 18 грудня 2013 № 939 «Порядок організації та забезпечення режиму секретності в державних органах, органах місцевого самоврядування, підприємствах, в установах і організаціях».

Навчальний контент

5. Методика опанування навчальної дисципліни (освітнього компонента)

Методика опанування навчальної дисципліни (освітнього компонента) передбачає висвітлення інформації за розділами, темами про всі навчальні заняття (лекції, практичні, семінарські, лабораторні) та надання рекомендацій щодо їх засвоєння (наприклад, у формі календарного плану чи деталізованого опису кожного заняття та запланованої роботи).

Види самостійної роботи (підготовка до аудиторних занять. Проведення розрахунків за первинними даними, отриманими на лабораторних заняттях, розв'язок задач, написання реферату, виконання розрахункової роботи, тощо).

Структура кредитного модуля

Номери, назви розділів, тем і питання навчальних занять, посилання на літературу		Кількість годин				
		Всього	у тому числі			
			Лекції	Практичні (семінарські) заняття	Лабораторні заняття (комп'ютерний практикум)	СР
Розділ (змістовий модуль) 1. Технічний захист інформації						
Тема 1	**Інформація як об'єкт захисту та технічний захист інформації**	**4**	**2**	**0**	**0**	**2**
Заняття 1/1	Лекція. Інформація як об'єкт захисту та технічний захист інформації. 1. Інформація як об'єкт захисту. Основні визначення та положення. 2. Технічний захист інформації. Основні визначення та положення. Основна література: [1-2]	**4**	2			2
Тема 2.	**Технічні канали витоку інформації, їх різновиди та сутність**	**20**	**4**	**2**	**4**	**10**
Заняття 2/1	Лекція. Технічні канали витоку інформації та їх класифікація. 1. Основні поняття з витоку інформації. 2. Класифікація технічних каналів витоку інформації. Основна література: [1-2]	**4**	**2**			**2**
Заняття 2/2	Лекція гр. Технічні канали витоку інформації, що утворюються від основних технічних засобів і систем. 1. Електромагнітні канали витоку інформації.	**4**	2			2

	2. Технічні канали витоку інформації через допоміжні технічні засоби та системи та сторонні провідники. 3. Електричні канали витоку інформації. 4. Параметричні канали витоку інформації, що обробляються в основних технічних засобах та системах. Основна література: [1-2]					
Заняття 2/3	Практичне. Технічні канали витоку мовної інформації. 1. Акустичні канали витоку інформації. 2. Акустично-вібраційні канали витоку інформації. 3. Акустично-електричні канали витоку інформації. 4. Акустично-оптичні канали витоку інформації. 5. Параметричні канали витоку мовної інформації. Основна література: [1-2]	**4**		2		**2**
Заняття 2/4	Лабораторна. Витік інформації через засоби прихованого добування інформації. 1. Сутність та класифікація засобів несанкціонованого перехоплення інформації. 2. Загальні характеристики засобів та сутність типових закладних пристроїв. (Радіозакладні пристрої, закладні пристрої типу довге вухо, закладні пристрої з надлишковим випромінюванням, мережеві закладні пристрої). 3. Напрямки захисту від закладних пристроїв. Основна література: [1-2]	**4**			2	2
Заняття 2/5	Лабораторна. Витік інформації в каналах зв'язку, витік відеоінформації та матеріально речовинні канали витоку. 1. Витік інформації в каналах зв'язку. 2. Витік видової інформації. 3. Матеріально речовинні канали витоку інформації. Способи добування інформації з магнітних носіїв. Основна література: [1-2]	**4**			2	2
Тема 3	**Базові регламентуючі положення в сфері технічного захисту інформації в Україні.**	**54**	**4**	**16**	**8**	**26**
Заняття 3/1	Лекція. Основні положення в сфері технічного захисту інформації в Україні	**4**	2			2

	1. Положення про технічний захист інформації в Україні. 2. Контроль за функціонуванням Положення про технічний захист інформації в Україні. Основна література: [3]					
Заняття З/2	Лекція. Положення про державну експертизу в сфері технічного захисту інформації. 1. Положення про державну експертизу в сфері технічного захисту інформації. 2. Положення про службу захисту інформації. Основна література: [3]	**4**	2			2
Заняття З/3	Практичне. Створення комплексів технічного захисту інформації на об'єктах інформаційної діяльності. 1. Захист інформації на об'єктах інформаційної діяльності. 2. Створення комплексу технічного захисту інформації. 3. Передпроектні роботи НД ТЗІ 3.1-001-07 Основна література: [3]	**6**		**4**		**2**
Заняття З/4	Практичне. Проведення перед проектних досліджень на об'єкті інформаційної діяльності. 1. Основні положення перед проектних досліджень на об'єкті інформаційної діяльності. 2. Основні етапи проведення перед проектних досліджень. Основна література: [3]	**6**		**4**		**2**
Заняття З/5	Практичне. Розроблення технічного завдання на виконання робіт із створення комплексу захисту на об'єкті інформаційної діяльності. 1. Порядок розроблення технічного завдання. 2. Вимоги до змісту розділів технічного завдання. Основна література: [3]	**6**		**4**		**2**
Заняття З/6	Практичне. Перехоплення даних. Класифікація каналів витоку інформації. Технічні канали витоку інформації. 1. Основні причини виникнення електричних каналів витоку інформації. 2. Порушники інформаційної безпеки та їх класифікація. 3. Перехоплення даних та канали витоку інформації. (Піранья ST-031) Основна література: [3]	**8**		**4**		**4**

Заняття 3/7	Лабораторне. Моніторинг радіотехнічних каналів. 1. Доглядові портативні телевізійні системи. 2. Програмно-апаратні засоби моніторингу радіотехнічних каналів. (Піранья ST-031, радіолокатор NR-900, Tektronix RSA 306) 3. Основна література: [3]	**4**			**2**	**2**
Заняття 3/8	Лабораторне. Панорамні приймачі та нелінійні радіолокатори. 1. Панорамні приймачі 2. Нелінійні радіолокатори NR-900 Основна література: [3]	**6**			**2**	**4**
Заняття 3/9	Лабораторне. Виявлення та блокування засобів негласного отримання інформації 1. Виявлення та блокування засобів негласного отримання інформації на об'єктах інформаційної діяльності. (Tektronix RSA 306) 2. Методика виявлення джерел акустичної або відеоінформації. (VEGA 09., Піранья ST 031, Flir i5) Основна література: [3]	**4**			**2**	**2**
Заняття 3/10	Лабораторне. Проведення комплексу організаційних і технічних заходів з обстеження приміщень з метою виявлення технічних каналів витоку інформації. 1. Розгортання та застосування аналізатора спектру Tektronix RSA 306. 2. Розгортання та застосування аналізатора спектру Піранья ST 031, (VEGA 09., тепловізор Flir i5) Основна література: [3]	**6**			**2**	**4**
Тема 4	**Методи та засоби захисту технічних каналів від витоку інформації на об'єктах інформаційної діяльності.**	**34**	**4**	4	**8**	**18**
Заняття 4/1	Лекція. Класифікація технічних каналів витоку інформації. Перехоплення даних. 1. Захист інформації від витоку технічними каналами. 2. Принципи блокування технічних каналів витоку інформації. 3. Захист інформації від витоку через закладні пристрої. Основна література: [3]	**4**	2			2
Заняття 4/2	Лекція. Поняття інженерно-технічного захисту. Фізичні засоби захисту: охоронні системи, охоронне телебачення, охоронне освітлення та засоби охоронної	**4**	2			2

	сигналізації. 1. Поняття інженерно-технічного захисту. 2. Охоронне телебачення, охоронне освітлення та засоби охоронної сигналізації. 3. Захист елементів будинків і приміщень. Основна література: [3]					
Заняття 4/3	Практичне. Апаратні засоби захисту. Ключові елементи, персональні кодові карти, персональний ідентифікатор, пристрої розпізнавання голосу користувача чи форми його пальців. 1. Апаратні засоби захисту інформації. 2. Основи апаратного захисту. Класифікація технічних засобів зняття інформації Основна література: [3]	**8**		4		4
Заняття 4/4	Лабораторна. Комплексні спеціальні перевірки, пошукові заходи та засоби. 1. Основні завдання комплексних спеціальних перевірок. 2. Класифікація закладних пристроїв та їх демаскуючі ознаки. 3. Технічні засоби пошуку засобів негласного знімання інформації. Основна література: [3]	**4**			2	2
Заняття 4/5	Лабораторне. Закладні пристрої, їх основні характеристики та застосування. Способи та засоби боротьби. 1. Класифікація закладних пристроїв. 2. Основні характеристики закладних пристроїв. 3. Структура радіоканалів витоку інформації Основна література: [3]	**4**			2	2
Заняття 4/6	Лабораторне. Закладні пристрої, їх основні характеристики та застосування. Способи та засоби боротьби. 1. Класифікація радіоканалів витоку інформації. 2. Класифікація акустичних каналів. 3. Класифікація пристроїв несанкціонованого зняття інформації. Основна література: [3]	**6**			2	4
Заняття 4/7	Лабораторна. Способи та засоби боротьби з закладними пристроями.	**4**			2	2

	1. Побічні електромагнітні випромінювання та наведення. 2. Методи виявлення пристроїв несанкціонованого зняття інформації Основна література: [3]					
Тема 5.	**Технічний захист інформації на мережевому рівні.**	**30**	**4**	**4**	16	**16**
Заняття 5/1	Лекція. Технічний захист інформації на мережевому рівні. 1. Міжмережеві екрани. 2. Технічний захист інформації від несанкціонованого доступу на апаратному рівні. 3. Система виявлення вторгнень. Основна література: [10, 20, 31, 32, 34, 35]	**4**	2			2
Заняття 5/2	Лекція. Системи технічного захисту інформації в Україні: стан, проблемні питання та напрями розвитку. 1. Проблеми захисту інформації в Україні. 2. Правові та нормативно-методичні проблеми. 3. Проблеми метрології та регламенту в системі ТЗІ. Основна література: [4]	**4**	2			2
Заняття 5/3	Лабораторне. Засоби технічного захисту інформації на ринку України та дозвіл користування ними. 1. Класифікатор засобів технічного захисту інформації НД ТЗІ 1.5-002-2012. 2. Основні положення, терміни та визначення. 3. Перелік та класифікація основних засобів технічного захисту інформації. Основна література: [4]	**4**			2	2
Заняття 5/4	Лабораторне. Зміст і послідовність робіт з підготовки та проведення комплексних спеціальних перевірок приміщень. 1. Мета проведення спеціальної комплексної перевірки приміщень. 2. Етапи виконання перевірки. 3. Пошук закладних пристроїв з радіочастотним каналом передачі на основі радіомоніторингу. Основна література: [4]	**6**			2	4
Заняття 5/5	Лабораторне. Локалізація місця розташування радіовипромінювальних закладних пристроїв за допомогою пошукового приладу ST 031 «Піранья».	**4**			2	2

	1. Підготовка контрольованого приміщення. 2. Методи пошуку: - амплітудний метод пошуку; - метод пошуку «акустичної зав'язки». Основна література: [4]					
Заняття 5/6	Практичне. Перевірка телефонних ліній. 1. Пошук закладних пристроїв, що використовують провідні комунікації. 2. Пошук закладних пристроїв, що використовують низькочастотні магнітні випромінювання. 3. Пошук сигналів і локалізація джерел. Основна література: [4]	**8**		4		4
Разом за розділом 1		**142**	**18**	**26**	**26**	**72**
Залік		**8**		**2**		**6**
Всього годин		**150**	**18**	**28**	**26**	**78**

6. Самостійна робота курсанта

Головними видами самостійної роботи курсантів є: самостійна підготовка до аудиторних занять та самостійна підготовка до екзамену.

Доцільно час самостійної підготовки для поглибленого вивчення та закріплення навчального матеріалу розподілити наступним чином:

№ з/п	Назва теми та перелік основних питань (перелік дидактичного забезпечення, посилання на літературу)	Кількість годин СР
1	Тема 1. Інформація як об’єкт захисту та технічний захист інформації 1. Інформація як об’єкт захисту та технічний захист інформації. Дидактичні засоби: методична розробка. Література: основна [1-2], допоміжна [1-8].	2
2	Тема 2. Технічні канали витоку інформації, їх різновиди та сутність 1. Технічні канали витоку інформації та їх класифікація. 2. Технічні канали витоку інформації, що обробляються в основних технічних засобах та системах. 3. Технічні канали витоку мовної інформації. 4. Виток інформації через засоби прихованого добування інформації. 5. Виток інформації в каналах зв’язку, виток видової інформації та матеріально речовинні канали витоку. Дидактичні засоби: методична розробка. Література: основна [1-2], допоміжна [9-10].	10

3	Тема 3. Базові регламентуючі положення в сфері технічного захисту інформації в Україні. 1. Положення про технічний захист інформації в Україні. 2. Положення про державну експертизу в сфері технічного захисту інформації. 3. Положення про службу захисту інформації. 4. Створення комплексів технічного захисту інформації на об'єктах інформаційної діяльності. 5. Основні положення перед проектних досліджень на об'єкті інформаційної діяльності. 6. Вимоги до змісту розділів технічного завдання. Перехоплення даних. 7. Класифікація каналів витоку інформації. 8. Основні причини виникнення електричних каналів витоку інформації. 9. Перехоплення даних та канали витоку інформації. Програмно-апаратні засоби моніторингу радіотехнічних каналів. Піранья ST-031, радіолокатор NR-900, Tektronix RSA 306. Дидактичні засоби: методична розробка. Література: основна [3], допоміжна [11].	26
4	Тема 4. Методи та засоби захисту технічних каналів від витоку інформації на об'єктах інформаційної діяльності. 1. Захист інформації від витоку технічними каналами. 2. Принципи блокування технічних каналів витоку інформації. 3. Захист інформації від витоку через закладні пристрої. 4. Поняття інженерно-технічного захисту. 5. Охоронне телебачення, охоронне освітлення та засоби охоронної сигналізації. 6. Захист елементів будинків і приміщень. 7. Апаратні засоби захисту інформації. 8. Основи апаратного захисту. Класифікація технічних засобів зняття інформації 9. Основні завдання комплексних спеціальних перевірок. 10. Класифікація закладних пристроїв та їх демаскуючі ознаки. 11. Технічні засоби пошуку засобів негласного знімання інформації. 12. Класифікація закладних пристроїв. 13. Основні характеристики закладних пристроїв. 14. Структура радіоканалів витоку інформації 15. Класифікація радіоканалів витоку інформації. 16. Класифікація акустичних каналів. 17. Класифікація пристроїв несанкціонованого зняття інформації. 18. Побічні електромагнітні випромінювання та наведення. 19. Методи виявлення пристроїв несанкціонованого зняття інформації. Дидактичні засоби: методична розробка. Література: основна [3], допоміжна [11].	18

5	Тема 5. Технічний захист інформації на мережевому рівні. 1. Міжмережеві екрани. 2. Технічний захист інформації від несанкціонованого доступу на апаратному рівні. 3. Система виявлення вторгнень. 4. Проблеми захисту інформації в Україні. 5. Правові та нормативно-методичні проблеми. 6. Проблеми метрології та регламенту в системі ТЗІ. 7. Класифікатор засобів технічного захисту інформації 8. НД ТЗІ 1.5-002-2012. 9. Основні положення, терміни та визначення. 10. Перелік та класифікація основних засобів технічного захисту інформації. 11. Мета проведення спеціальної комплексної перевірки приміщень. 12. Етапи виконання перевірки. 13. Пошук закладних пристроїв з радіочастотним каналом передачі на основі радіомоніторингу. 14. Підготовка контрольованого приміщення. 15. Методи пошуку: - амплітудний метод пошуку; - метод пошуку «акустичної зав'язки». 16. Пошук закладних пристроїв, що використовують провідні комунікації. 17. Пошук закладних пристроїв, що використовують низькочастотні магнітні випромінювання. 18. Пошук сигналів і локалізація джерел. Дидактичні засоби: методична розробка. Література: основна [4], допоміжна [11].	16
6	Залік	6

Політика та контроль

7. Політика навчальної дисципліни (освітнього компонента)

Політика навчальної дисципліни визначає систему вимог, які викладач ставить перед курсантом:

правила відвідування занять (як лекцій, так і практичних/лабораторних);

правила поведінки на заняттях (активність, підготовка коротких доповідей, використання засобів зв’язку тощо);

правила призначення заохочувальних та штрафних балів;

політика дедлайнів та перескладань;

політика академічної доброчесності.

8. Види контролю та рейтингова система оцінювання результатів навчання (РСО)

1. Рейтинг курсанта з кредитного модуля (далі – *RD)* розраховується зі 100 балів, стартовий рейтинг (протягом семестру) складається з балів, що він отримує:

- в результаті поточного контролю на практичних заняттях (2 усні відповіді);
- за виконання контрольних робіт (4 експрес-контролі);
- за ведення конспекту на лекційному занятті (15 лекційних занять з головних питань кредитного модулю);
- в результаті оцінювання його активності у навчанні за шкалою заохочувальних (штрафних) балів (не є обов’язковим для визначення стартового рейтингу кожного курсанта).

2. Критерії нарахування балів.

2.1. Поточний контроль на практичних заняттях (2 усні відповіді).

Ваговий бал усної відповіді – 5 балів. Кількість балів за 2 усні відповіді складає: 15 *балів* х 2 відповіді = 30 *балів.*

2.2. Виконання контрольних робіт (4 експрес-контролі).

Ваговий бал письмової відповіді на питання контрольної роботи (експрес-контролю) - 5 балів. Контрольна робота (експересс-контроль) тривалістю 10 хв., під час проведення практичного заняття. Максимальна кількість балів за контрольні роботи (експрес-контролі) складає: 10 *балів* х 4 = 40 *балів.*

Критерії нарахування балів за усну відповідь на практичних заняттях, контрольній роботі

- "відмінно" - повна відповідь (не менше 90% потрібної інформації) – 14 -15 балів;

"добре" - достатньо повна (не менше 75% потрібної інформації) або повна відповідь з незначними неточностями – 11 – 13 балів;

- "задовільно" - неповна відповідь (не менше 60% потрібної інформації) та має незначні помилки – 9 – 10 балів;
- "незадовільно" - відповідь не відповідає вимогам для оцінювання на «задовільно» – 0 балів.

2.3. Ведення конспекту на лекційному занятті (15 лекційних занять з головних питань кредитного модулю).

Ваговий бал ведення конспекту на лекційному занятті – 2 бали. Максимальна кількість балів за ведення конспекту на лекційних заняттях з головних питань кредитного модулю складає: 2 *бали* х 15 = 30 *балів.*

Заохочувальні та штрафні бали.

Сума як штрафних, так і заохочувальних балів складає 0,1 r_c = ± 10 балів та вибірково може бути нарахована за:

- активність на заняттях та систематична самостійна робота протягом семестру: +1… +10;
- участь в олімпіадах, ВНО та наукових конференціях, виконання завдань із удосконалення методичних та дидактичних матеріалів з дисципліни +1…+ 10;
- пасивність на заняттях та несистематична самостійна робота протягом семестру: -1… – 10;

Заохочувальні та штрафні бали застосовуються вибірково та мають на меті підвищення мотивації курсантів до активної, відповідальної, системної роботи на заняттях протягом семестру.

3. Календарна атестація курсантів проводиться відповідно до Графіка-календаря освітнього процесу ІСЗЗІ КПІ ім. Ігоря Сікорського на навчальний рік, з кредитного модуля викладачами за результатами поточного рейтингу курсанта на час атестації. Якщо значення цього рейтингу не менше 50 % від максимально можливого на час атестації, курсант вважається атестованим.

4. Умовою допуску до заліку є отримання курсантом позитивних оцінок з усних відповідей на практичні заняття, контрольних робіт.

При цьому вважається, що курсант не виконав програму начальної дисципліни та потребує додаткових занять за окремим планом для підвищення рейтингу до необхідного рівня.

5. На заліку курсант виконує залікову письмову контрольну роботу. Порядок виконання та критерії оцінювання відповіді визначаються Методичними рекомендаціями щодо проведення заліку з семестрового модулю Системи та комплекси технічного захисту інформації. На залік виноситься 72 питання. В кожному білеті три питання, перше та друге теоретичне, максимум по 25 балів, третє практичне, максимум 50 балів. Відповідно максимальний бал за залік 100 балів.

Критерії нарахування балів за відповідь на теоретичне питання:

- "відмінно" - повна відповідь (не менше 90% потрібної інформації) – 23 - 25 балів;

- “добре” - достатньо повна (не менше 75% потрібної інформації) або повна відповідь з незначними неточностями – 19 – 22 бали;

- «задовільно” - неповна відповідь (не менше 60% потрібної інформації) та має незначні помилки – 15 – 18 балів;

- “незадовільно» - відповідь не відповідає вимогам для оцінювання на «задовільно» – 0 балів.

Критерії нарахування балів за виконння завдання по практичному питанню:

- “відмінно” - повна відповідь (не менше 90% потрібної інформації) – 45 - 50 балів;

- “добре” - достатньо повна (не менше 75% потрібної інформації) або повна відповідь з незначними неточностями –38 – 44 бали;

- “задовільно” - неповна відповідь (не менше 60% потрібної інформації) та має незначні помилки – 30 – 37 балів;

- “незадовільно” - відповідь не відповідає вимогам для оцінювання на «задовільно» – 0 балів.

6. Вважається, що курсант успішно виконав навчальну програму навчальної дисципліни, якщо він отримав позитивну загальну рейтингову оцінку $RD \geq 60$.

Рейтингова оцінка трансформується до університетської системи оцінювання згідно з таблицею 1.

Таблиця 1. Переведення рейтингових балів до оцінок за університетською шкалою
Рейтингові бали, RDОцінка за університетською шкалою

Кількість балів	оцінка
95-100	Відмінно
85-94	Дуже добре
75-84	Добре
65-74	Задовільно
60-64	Достатньо
менше 60	Незадовільно

9. Додаткова інформація з навчальної дисципліни

Перелік питань, які виносяться на залік:

1. Сучасні методи несанкціонованого знімання інформації. Класифікація технічних засобів знімання інформації та їх призначення.
2. Призначення, принцип дії та можливості щодо зняття акустичної інформації з використанням акустичних приймачів та диктофонів.
3. Призначення, принцип дії та можливості щодо зняття акустичної інформації лазерними засобами підслуховування.
4. Призначення, принцип дії та можливості щодо зняття акустичної інформації засобами високочастотного нав’язування.
5. Сутність несанкціонованого знімання мовної інформації через закладні пристрої. Загальна класифікація закладних пристроїв.
6. Радіозакладні пристрої, принципи функціонування та їх загальні характеристики.
7. Закладні пристрої з передачею інформації через мережу живлення, принципи функціонування та загальні характеристики.
8. Закладні пристрої, що реалізують методи високочастотного нав'язування, принципи функціонування та загальні характеристики.
9. Призначення та класифікація технічних засобів негласного оптичного спостереження.
10. Призначення, принцип дії та можливості щодо зняття інформації із застосуванням оптичних систем та візуально-оптичних приладів.

11. Призначення, принцип дії та можливості щодо зняття інформації із застосуванням засобів телевізійного спостереження (прихованих відеокамер).

12. Призначення, принцип дії та можливості щодо зняття інформації із застосуванням технічних засобів спостереження в інфрачервоному та радіодіапазонах.

13. Призначення, принцип дії та можливості перехоплення сигналів радіоприймачами.

14. Призначення, принцип дії та можливості перехоплення сигналів технічними засобами аналізу сигналів.

15. Призначення, принцип дії та можливості технічних засобів визначення координат та джерел радіосигналів.

16. Призначення, принцип дії та можливості технічних засобів перехоплення оптичних та електричних сигналів.

17. Загальний порядок проведення спеціальних досліджень, види контрольно-вимірювальних та пошукових робіт, категорії технічних засобів контролю та пошуку, що використовуються під час проведення спец досліджень об'єктів інформаційної діяльності.

18. Загальний порядок проведення спеціальних досліджень, види контрольно-вимірювальних та пошукових робіт, категорії технічних засобів контролю та пошуку, що використовуються під час проведення спец досліджень ОТЗ та ДТЗС.

19. Інструментальний контроль захищеності інформації на ОІД та об'єктах ОЕТ, завдання та загальний порядок його проведення.

20. Загальний порядок проведення інструментального контролю, види контрольно-вимірювальних та пошукових робіт, категорії технічних засобів контролю та пошуку, що використовуються під час інструментального контролю захищеності інформації на ОІД та об'єктах ОЕТ, де обробляється інформація технічними засобами.

21. Класифікація та призначення технічних засобів, систем та комплексів ТЗІ, що використовуються під час проведення спецдосліджень ОІД, ОТЗ, ДТЗС та інструментального контролю захищеності інформації від витоку технічними каналами.

22. Призначення, склад, принцип дії та можливості індикаторів електромагнітних випромінювань. Призначення та можливості аналізатора електромагнітного поля "Кордон".

23. Призначення, склад, принцип дії та можливості індикаторів електромагнітних випромінювань. Призначення та можливості універсального приладу ST-31M "Піранья".

24. Призначення, склад, принцип дії та можливості радіочастотомірів. Призначення та можливості пошукового виробу "РИЧ-3".

25. Призначення, склад, принцип дії та можливості радіочастотомірів. Призначення та можливості портативного багатофункціонального частотоміру 3000A+.

26. Призначення, склад, принцип дії та можливості приймачів для сканування. Призначення та можливості портативного приймача "Скорпіон" ("Скорпіон-XL"), що сканує.

27. Призначення, склад, принцип дії та можливості приймачів для сканування. Призначення та можливості портативного приймача AR-3000A, що сканує.

28. Призначення, склад, принцип дії та можливості приймачів для сканування. Призначення та можливості портативного професійного приймача AR-ONE, що сканує.

29. Призначення, склад, принцип дії та можливості аналізаторів спектру. Призначення та можливості аналізатора спектру GSP-810 (GSP-827);

30. Призначення, склад, принцип дії та можливості аналізаторів спектру. Призначення та можливості пошукового аналізатора спектру SpektrumJet.

31. Призначення, склад, принцип дії та можливості спеціальних осцилографів. Призначення та можливості спеціального осцилографа HAMEG HMO 2022.

32. Призначення, склад, принцип дії та можливості селективних мікровольтметрів (нановольтметрів). Призначення та можливості селективного мікровольтметра SMV-8,5.

33. Призначення, склад, принцип дії та можливості селективних мікровольтметрів (нановольтметрів). Призначення та можливості селективного нановольтметра Unipan 237.

34. Призначення, склад, принцип дії та можливості нелінійних локаторів. Призначення та можливості нелінійного радіолокатора NR-900EM.

35. Призначення, склад, принцип дії та можливості нелінійних локаторів. Призначення та можливості дводіапазонного нелінійного радіолокатора “Лорнет-0836”.

36. Призначення, класифікація та загальна характеристика сучасних автоматизованих пошукових комплексів. Принципи функціонування автоматизованих комплексів.

37. Призначення, класифікація та загальна характеристика сучасних автоматизованих пошукових комплексів. Загальна характеристика спеціального програмного забезпечення автоматизованих комплексів.

38. Призначення, склад та можливості пошукового автоматизованого програмно-апаратного комплексу DigiScan EX Standard (DigiScan EX Professional).

39. Призначення, склад та можливості пошукового автоматизованого програмно-апаратного комплексу виявлення радіо випромінюючих засобів та радіомоніторингу «Крона-плюс».

40. Призначення та принцип дії металодетекторів. Характеристики та можливості металодетектора “Сфінкс ВМ-311”.

41. Призначення та принцип дії тепловізорів. Призначення та можливості професійного тепловізору Flir серії P.

42. Призначення та принцип дії приладів рентген візуального контролю. Характеристика та можливості портативного рентген телевізійного комплексу Flat Scan 27.

43. Призначення та принцип дії ендоскопів. Характеристики та можливості ендоскопу “Кобра-ТВ”.

44. Призначення та принцип дії технічних засобів радіаційного контролю. Призначення та можливості дозиметру цифрового ДКГ-АТ-2503.

45. Класифікація та призначення технічних засобів, систем та комплексів ТЗІ, що використовуються під час створення комплексів ТЗІ на ОІД та об’єктах ЕОТ.

46. Технічні засоби захисту систем електроживлення. Призначення та можливості застосування трансформаторів розділових з екранованою обмоткою “РІАС-ТР/2” (“РІАС-ТР/5”, “РІАС-ТР/10”).

47. Технічні засоби захисту систем електроживлення. Призначення та можливості застосування фільтрів мережевих загороджувальних високих частот “РІАС-4ФМ/10,20”.

48. Технічні засоби захисту систем електроживлення. Призначення та можливості застосування генератору електромагнітного шуму мережевого “Базальт-2ГС”.

49. Організація захисту мовної інформації у виділеному приміщенні. Призначення на принципи дії пасивних та активних засобів захисту мовної інформації.

50. Призначення, технічні характеристики та можливості застосування випромінювачів шуму та вібрацій “РІАС-2ГС” (“РІАС-2ГМ”).

51. Призначення та принцип дії технічного засобу запобігання витоку мовної інформації каналами “ВЧ нав’язування”. Призначення та можливості застосування пристрою високочастотної перешкоди “Гром-ЗИ-6”, що маскує.

52. Характеристика каналів витоку інформації при експлуатації АС та засобів ОТ та напрямки роботи із забезпечення захисту інформації.

53. Призначення, склад, характеристики та можливості захищеного автоматизованого робочого місця “ЕПОС Межа” (Україна).

54. Призначення, склад, характеристики та можливості захищеного автоматизованого робочого місця “Плазма-3В-АРМ”.

55. Призначення, склад, та можливості апаратно-програмного комплексу “Рубіж”.

56. Призначення, склад, та можливості апаратно-програмного комплексу “Лоза”.

57. Призначення та принципи функціонування систем криптографічного захисту інформації. Призначення та основні характеристики шифратора з інтегрованим модулем комутації “Гном-Е” (В-271-Е).

58. Призначення та принципи функціонування систем криптографічного захисту інформації. Призначення та основні характеристики шифратора з інтегрованим модулем комутації “Пелена-Е” (В-371-Е).

59. Перелік заходів захисту інформації в АС і ЗОТ від витоку каналами ПЕМВН. Загальні рекомендації щодо застосування системи просторового зашумлення об’єктів ЕОТ.

60. Призначення, склад, характеристики та умови застосування генераторів електромагнітного поля шуму “Базальт 5ГЕШ”.

61. Призначення КСЗІ. Суб’єкти та об’єкти КСЗІ.

62. Етапи створення КСЗІ.

63. Порядок формування загальних вимог до КСЗІ в ІТС (1 етап).

64. Порядок розробки політики безпеки (ПБ) інформації в ІТС (2 етап).

65. Порядок розробки технічного завдання (ТЗ) на створення КСЗІ (3 етап).

66. Порядок введення КСЗІ в дію та оцінювання захищеності інформації в ІТС (5 етап).

67. Супровід КСЗІ (6 етап).

68. Загальні положення щодо створення та атестації КТЗІ. НДТЗІ 3.6-003-2016.

69. Передпроектні роботи розроблення КТЗІ. НДТЗІ 3.6-003-2016.

70. Розроблення технічного проекту комплексу ТЗІ. НДТЗІ 3.6-003-2016.

71. Упровадження комплексу ТЗІ. НДТЗІ 3.6-003-2016.