МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Львівський національний університет імені Івана Франка
Факультет прикладної математики та інформатики
Кафедра кібербезпеки

Затверджено
На засіданні кафедри кібербезпеки
факультету прикладної математики та
інформатики
Львівського національного університету
імені Івана Франка
(Протокол № 15/23 від 29 серпня 2023 р.)

Завідувач кафедри

Венгерський П.С.

Силабус з навчальної дисципліни

"Методи та засоби технічного захисту інформації",

що викладається в межах ОПП Кібербезпека

першого (бакалаврського) рівня вищої освіти для здобувачів

зі спеціальності 125 – Кібербезпека та захист інформації

Львів - 2023

Назва дисципліни	Методи та засоби технічного захисту інформації
Адреса викладання дисципліни	м. Львів, вул. Університетська 1
Факультет та кафедра, за якою закріплена дисципліна	Факультет прикладної математики та інформатики Кафедра кібербезпеки
Галузь знань, шифр та назва спеціальності	12 – інформаційні технології 125 – кібербезпека та захист інформації
Викладачі дисципліни	Пархуць Любомир Теодорович, д.т.н., професор кафедри кібербезпеки;
Контактна інформація викладачів	Liubomyr.Parkhuts@lnu.edu.ua; Головний корпус ЛНУ ім. І. Франка, каб. 380. м. Львів, вул. Університетська, 1
Консультації з питань навчання по дисципліні відбуваються	Консультації в день проведення лекцій/практичних занять (а також за розкладом консультацій кафедри).
Сторінка курсу	https://ami.lnu.edu.ua/course/pentest
Інформація про дисципліну	Дисципліна "Методи та засоби технічного захисту інформації" є нормативною дисципліною зі спеціальності 125 – кібербезпека та захист інформації для освітньої програми Кібербезпека, яка викладається в 7-му семестрі в обсязі 6 кредитів (за Європейською Кредитно-Трансферною Системою ECTS).
Коротка анотація дисципліни	Курс спрямований на формування у студентів професійних компетентностей, розвиток системи знань про методи і засоби захисту інформації від витоку через технічні канали при її обробці технічними засобами, а також методів і засобів захисту акустичної (мовної) інформації.
Мета та цілі дисципліни	Метою курсу нормативної дисципліни є формування у студентів теоретичної та практичної бази знань про методи і засоби захисту інформації від витоку через технічні канали при її обробці технічними засобами, а також методів і засобів захисту акустичної (мовної) інформації.
Література для вивчення дисципліни	1. Пархуць Л.Т., Костяк М.Ю. Методи і засоби захисту інформації. Конспект лекцій. Частина 1. "Захист інформації від витоку по технічних каналах". НУ"ЛП", – Львів, – 2023. – 84 с. 2. Пархуць Л.Т., Костяк М.Ю. Методи і засоби захисту інформації. Конспект лекцій. Частина 2. "Методи і засоби пошуку електронних пристроїв перехоплення інформації". НУ"ЛП", – Львів, – 2023. – 80 с. 3. Методичні вказівки та інструкції до виконання лабораторних робіт з курсу "Методи і засоби захисту інформації". Укладачі: М.Ю.Костяк, Л.Т.Пархуць. Львів – 2023. 4. Пономаренко В. С. Основи захисту інформації. Навчальний посібник / В.С.Пономаренко, І.В.Журавльова. – Харків: Вид. ХДЕУ, 2021. – 176 с. 5. Юдін О.К. Захист інформації в мережах передачі даних / О.К. Юдін, О.Г. Корченко, Г.Ф. Конахович // Підручник — К. : Вид-во DIRECTLINE, – 2019. – 714 с. 6. Домарєв В. В. Безпека інформаційних технологій. Методи створення

	систем захисту / В.В. Домарєв. – К.: ТзОВ ТІД ДС, – 2021. – 688 с. 7. Лаптєв О.А., Савченко В.А., Шуклін Г.В. Виявлення та блокування засобів негласного отримання інформації на об'єктах інформаційної діяльності. – Київ. Видавництво ДУТ, – 2020, – 126 с. Додаткова література: 8. Закон України "Про державну таємницю": Закон України від 21.09.99 № 1079-XIV // Відомості Верховної Ради України. – 1999. – № 49. – Ст. 428. 9. Про інформацію: Закон України від 02.10.92 № 2657-XII // Відомості Верховної Ради України. – 1992. – № 48. – Ст. 650. 10. Архипов О.Є., Бородавко І.Т., Ворожко В.П. Оцінювання ефективності системи охорони державної таємниці: Монографія. – К.: Наук.-вид. відділ НА СБ України, – 2017. – 63 с. 11. Антонюк А.О. Основи захисту інформації в автоматизованих системах / А. О. Антонюк. – К.: КМ Академія, – 2016. – 244 с. 12. Вербіцький О.В. Вступ до криптології / О.В.Вербіцький. – Львів: Вид-во НТЛ, – 2018. – 248 с. 13. ДСТУ 3396.2–97. Захист інформації. Технічний захист інформації. Терміни і визначення. – К.: Держстандарт України, – 1998. 14. Генне В.І. Захист інформації від витоку через побічні електромагнітні випромінювання цифрового електромагнітного устаткування // Захист інформації. – 2018. № 2. – С. 89-95. 15. Максименко Г.А., Хорошко В.О. Методи виявлення, обробки та ідентифікації сигналів радіозакладних пристроїв. – К.: ООО "ПоліграфКонсалтинг", 2014. – 317с. 16. Хорошко В.О., Чекатков А.А. Методи та засоби захисту інформації. – К.: Видавництво "ЮНІОР", 2013. –504 с. 17. http://www.dstszi.gov.ua/dstszi/control/uk/index
Обсяг курсу	Загальний обсяг: 180 годин. Аудиторних занять: 64 год., з них 32 год. лекцій та 32 год. лабораторних робіт. Самостійної роботи: 116 год.
Очікувані результати навчання	У результаті вивчення навчальної дисципліни студент має набути таких компетентностей: **<u>знати:</u>** – основні форми представлення інформації; – проблеми захисту даних; – сигнали поширення та передачі інформації; – основі джерела та шляхи витоку інформації; – способи несанкціонованого перехоплення інформації; – основні технічні засоби, що використовуються для несанкціонованого перехоплення інформації; – методи та засоби захисту інформації; – основні технічні засоби, що використовуються для захисту інформації від несанкціонованого перехоплення. **<u>вміти:</u>** – аналізувати приміщення щодо можливих джерел та шляхів витоку інформації; – виконувати пошук засобів несанкціонованого перехоплення інформації; – користуватися технічними засобами, що використовуються для несанкціонованого перехоплення інформації; – виконувати захист приміщень від несанкціонованого перехоплення інформації.;

	Курс забезпечує набуття таких компетентностей: ІК, КЗ-1, КЗ-2, КЗ-3, КЗ-4, КЗ-5, КФ-1, КФ-2, КФ-3, КФ-5, КФ-6, КФ-8, КФ-10, КФ-12; **та програмних результатів навчання:** ПРН-1, ПРН-2, ПРН-3, ПРН-4, ПРН-6, ПРН-7, ПРН-10, ПРН-14 ПРН-15, ПРН-21, ПРН-23, ПРН-26, ПРН-38, ПРН-39, ПРН-31, ПРН-34, ПРН-36.
Ключові слова	Захист інформації, кібербезпека, загроза, вразливість, конфіденційність, цілісність, технічні канали витоку інформації, пасивні методи захисту інформації, активні методи захисту інформації.
Формат курсу	Очний

Підсумковий контроль, форма	Залік у кінці семестру
Навчальні методи та техніки, які будуть використовуватися під час викладання курсу	Презентації, лекції. Модульний контроль. Лабораторні роботи (теми лабораторних робіт приведені нижче).
Необхідне обладнання	Комп'ютер, чи ноутбук з можливістю віртуалізації; Нелінійний локатор, багатофункціональний комплекс "Піранья ST-31P", Скануйчий приймач Ar-8200, Програмний комплекс DigiScan, Виявляч відеокамер Hunter-827, Виявляч об'єктивів прихованих відеокамер Wega, Індикатор поля "Protect-1210".
Критерії оцінювання (окремо для кожного виду навчальної діяльності)	Оцінювання проводиться за 100-бальною шкалою. Бали нараховуються за наступним співвідношенням: • модульний контроль, тестування, усне опитування: 40% семестрової оцінки; максимальна кількість балів 40 • лабораторні роботи: 60% семестрової оцінки; максимальна кількість балів 60 Підсумкова максимальна кількість балів 100. **Академічна доброчесність**: Очікується, що роботи студентів будуть їх оригінальними дослідженнями чи міркуваннями. Відсутність посилань на використані джерела, фабрикування джерел, списування, втручання в роботу інших студентів становлять, але не обмежують, приклади можливої академічної недоброчесності. Виявлення ознак академічної недоброчесності в письмовій роботі студента є підставою для її незарахуванння викладачем, незалежно від масштабів плагіату чи обману. **Відвідання занять** є важливою складовою навчання. Очікується, що всі студенти відвідають усі лекції та практичні зайняття курсу. Студенти повинні інформувати викладача про неможливість відвідати заняття. У будь-якому випадку студенти зобов'язані дотримуватися термінів визначених для виконання всіх видів письмових робіт та індивідуальних завдань, передбачених курсом. **Література.** Уся література, яку студенти не зможуть знайти самостійно, буде надана викладачем виключно в освітніх цілях без права її передачі третім особам. Студенти заохочуються до використання також й іншої літератури та джерел, яких немає серед рекомендованих.

	Політика виставлення балів. Враховуються бали набрані при поточному тестуванні, самостійній роботі та бали підсумкового тестування. При цьому обов'язково враховуються присутність на заняттях та активність студента під час практичного заняття; недопустимість пропусків та запізнень на заняття; користування мобільним телефоном, планшетом чи іншими мобільними пристроями під час заняття в цілях не пов'язаних з навчанням; списування та плагіат; несвоєчасне виконання поставленого завдання і т. ін. Жодні форми порушення академічної доброчесності не толеруються.
Питання до контролю	1. Основні напрямки захисту інформації. 2. Основні форми представлення інформації: документальна, мовна, телекомунікаційна. 3. Основні об’єкти захисту інформації. 4. Технічні засоби прийому, обробки, збереження і передачі інформації (ТЗПІ). Допоміжні технічні засоби і системи (ДТЗС). 5. Об’єкт ТЗПІ. Поняття небезпечних зон. 6. Випадкові антени. Класифікація і характеристика технічних каналів витоку інформації. 7. Електромагнітні, електричні і параметричні канали. 8. Повітряні, вібраційні, електроакустичні, оптико-електронні канали. 9. Проектно-архітектурні рішення. 10. Проведення організаційних заходів. 11. Пасивні (контроль і обмеження доступу на об’єкти ТЗПІ, локалізація випромінювань, розв’язка інформаційних сигналів) та активні (просторове зашумлення, лінійне зашумлення, знищення закладних пристроїв) технічні заходи 12. Виявлення портативних електронних пристроїв перехоплення інформації (закладних пристроїв): спеціальні обстеження, спеціальна перевірка. 13. Пасивні та активні методи захисту. 14. Побічне електромагнітне випромінювання. 15. Екранування технічних засобів. Електростатичне екранування. Магнітостатичне екранування. Електромагнітне екранування. Схеми та вимоги до матеріалів екранування. 16. Заземлення технічних засобів. Основні вимоги до системи заземлення. 17. Опір заземлення. Питомий опір грунтів. 18. Матеріали для виконання заземлення. Виконання заземлення та захист від пошкоджень. 19. Фільтрація інформаційних сигналів. Роздільні трансформатори. 20. Завадопоглинаючі фільтри. Основні вимоги до захисних фільтрів. Конструктивне виконання та характеристики фільтрів. 21. Просторове і лінійне зашумлення. Основні вимоги до системи просторового зашумлення. 22. Системи "білий шум" та "синфазні завади". Генератори шуму, типи та основні характеристики. Ефективність просторового зашумлення. 23. Системи лінійного зашумлення та їх застосування. 24. Пасивні та активні методи і засоби захисту інформації. 25. Звукоізоляція приміщень. Основні вимоги та оцінка ефективності звукоізоляції. 26. Звукоізоляція дверей та вікон приміщення. Використання акустичних екранів. Матеріали, що використовуються для звукоізоляції.

	27. Звуковбирні властивості матеріалів та показники їх ефективності. Використання спеціальних кабін. 28. Акустичне маскування. Віброакустичне маскування. 29. Генератори акустичного шуму. Структура та основні характеристики систем активного віброакустичного маскування. Дотримання вимог охорони праці при використання активних засобів акустичного маскування приміщень. 30. Виявлення і придушення диктофонів і акустичних закладок. Детектори диктофонів. 31. Пристрої електромагнітного придушення диктофонів. Системи ультразвукового придушення диктофонів. Постійний радіоконтроль приміщень. 32. Встановлення прицільних радіозавад. Системи просторового електромагнітного зашумлення та завадопоглинаючі фільтри. 33. Особливості та шляхи перехоплення інформації з використанням телефонних ліній. 34. Пасивні та активні методи захисту. 35. Обмеження інформативних сигналів. 36. Фільтрація інформативних сигналів. Відключення джерел інформативних сигналів. 37. Лінійне зашумлення телефонних ліній. 38. Метод синфазної маскуючої НЧ завади. Метод ВЧ маскуючої завади. 39. Метод ультразвукової маскуючої завади. Метод підвищення напруги. 40. Метод "обнулення". Компенсаційний метод. Метод "випалювання". 41. Приклади технічної реалізації засобів для захисту телефонних ліній та їх характеристики. 42. Використання спеціальних електронних блокіраторів.
Опитування	Анкету-оцінку з метою оцінювання якості курсу буде надано після завершенню курсу.

Схема курсу
Лекційні заняття

№	Найменування розділів, тем, питань	Год
1	**Вступ.** Предмет дисципліни та її завдання. Зв'язок з іншими дисциплінами спеціальності. Важливість проблеми та необхідність захисту інформації від несанкціонованого доступу. Основні напрямки захисту інформації.	2
2	Частина 1. **Захист інформації від витоку по технічних каналах .** *Тема 1.* **Класифікація і характеристики методів і засобів захисту інформації від витоку по технічних каналах.** Основні форми представлення інформації: документальна, мовна, телекомунікаційна. Основні об'єкти захисту інформації. Технічні засоби прийому, обробки, збереження і передачі інформації (ТЗПІ). Допоміжні технічні засоби і системи (ДТЗС). Об'єкт ТЗПІ. Поняття небезпечних зон. Випадкові антени. Класифікація і характеристика технічних каналів витоку інформації.	4

№	Найменування розділів, тем, питань	Год
	Електромагнітні, електричні і параметричні канали. Повітряні, вібраційні, електроакустичні, оптико-електронні канали.	
3	*Тема 2.* **Класифікація методів і засобів захисту інформації від витоку по технічних каналах.** Проектно-архітектурні рішення. Проведення організаційних заходів. Пасивні (контроль і обмеження доступу на об'єкти ТЗПІ, локалізація випромінювань, розв'язка інформаційних сигналів) та активні (просторове зашумлення, лінійне зашумлення, знищення закладних пристроїв) технічні заходи. Виявлення портативних електронних пристроїв перехоплення інформації (закладних пристроїв): спеціальні обстеження, спеціальна перевірка.	6
4	*Тема 3.* **Методи і засоби захисту інформації ТЗПІ від витоку по технічних каналах.** Пасивні та активні методи захисту. Побічне електромагнітне випромінювання. Екранування технічних засобів. Електростатичне екранування. Магнітостатичне екранування. Електромагнітне екранування. Схеми та вимоги до матеріалів екранування. Заземлення технічних засобів. Основні вимоги до системи заземлення. Опір заземлення. Питомий опір грунтів. Матеріали для виконання заземлення. Виконання заземлення та захист від пошкоджень. Фільтрація інформаційних сигналів. Роздільні трансформатори. Завадопоглинаючі фільтри. Основні вимоги до захисних фільтрів. Конструктивне виконання та характеристики фільтрів. Просторове і лінійне зашумлення. Основні вимоги до системи просторового зашумлення. Системи "білий шум" та "синфазні завади". Генератори шуму, типи та основні характеристики. Ефективність просторового зашумлення. Системи лінійного зашумлення та їх застосування.	6
5	*Тема 4.* **Методи і засоби захисту мовної інформації.** Пасивні та активні методи і засоби. Звукоізоляція приміщень. Основні вимоги та оцінка ефективності звукоізоляції. Звукоізоляція дверей та вікон приміщення. Використання акустичних екранів. Матеріали, що використовуються для звукоізоляції. Звуковбирні властивості матеріалів та показники їх ефективності. Використання спеціальних кабін. Акустичне маскування. Віброакустичне маскування. Генератори акустичного шуму. Структура та основні характеристики систем активного віброакустичного маскування. Дотримання вимог охорони праці при використання активних засобів акустичного маскування приміщень. Виявлення і придушення диктофонів і акустичних закладок. Детектори диктофонів. Пристрої електромагнітного придушення диктофонів. Системи ультразвукового придушення диктофонів. Постійний радіоконтроль приміщень. Встановлення прицільних радіозавад. Системи просторового електромагнітного зашумлення та завадопоглинаючі фільтри.	6

№	Найменування розділів, тем, питань	Год
6	*Тема 5.* **Методи і засоби захисту телефонних ліній.** Особливості та шляхи перехоплення інформації з використанням телефонних ліній. Пасивні та активні методи захисту. Обмеження інформативних сигналів. Фільтрація інформативних сигналів. Відключення джерел інформативних сигналів. Лінійне зашумлення телефонних ліній. Метод синфазної маскуючої НЧ завади. Метод ВЧ маскуючої завади. Метод ультразвукової маскуючої завади. Метод підвищення напруги. Метод "обнулення". Компенсаційний метод. Метод "випалювання". Приклади технічної реалізації засобів для захисту телефонних ліній та їх характеристики. Використання спеціальних електронних блокіраторів.	6
	Всього за семестр	**32**

Лабораторні роботи

№	Назва лабораторної роботи	Год
		ДФН
1.	Дослідження каналу витоку інформації через коло заземлення та методи її захисту.	4
2.	Дослідження схем захисту від витоку інформації через коло електроживлення.	4
3.	Дослідження впливу електромагнітних і акустичних полів на ТЗПІ.	4
4.	Дослідження акустичної звукоізоляції приміщення.	4
5.	Пошук закладних пристроїв за допомогою нелінійного локатора.	4
6.	Дослідження генераторів шуму.	4
7.	Дослідження систем захисту телефонних ліній від несанкціонованого перехоплення інформації.	4
8.	Підсумкове заняття з лабораторного практикуму	4
	Всього за семестр	**32**