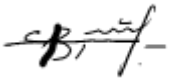
МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Львівський національний університет імені Івана Франка
Факультет прикладної математики та інформатики
Кафедра кібербезпеки

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 П.С.Венгерський

Силабус з навчальної дисципліни "Технічні канали витоку інформації", що викладається в межах ОПП Кібербезпека першого (бакалаврського) рівня вищої освіти для здобувачів з спеціальності 125 – кібербезпека та захист інформації

Львів 2023 р.

Назва дисципліни	**Технічні канали витоку інформації**
Адреса викладання дисципліни	Львівський національний університет імені Івана Франка, вул. Університетська 1, м. Львів, Україна, 79000
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	Щербина Микола Юрійович, асистент кафедри кібербезпеки (лекції та лабораторні заняття)
Контактна інформація викладачів	Mykola.Shcherbyna@lnu.edu.ua https://ami.lnu.edu.ua/employee/shcherbyna-m-yu; Головний корпус ЛНУ ім. І. Франка, каб. 380. м. Львів, вул. Університетська, 1
Консультації з питань навчання по дисципліні відбуваються	Консультації проводять раз на тиждень згідно з оприлюдненим розкладом консультацій викладача. Можливі онлайн консультації через Zoom чи Microsoft Teams. Для погодження часу онлайн консультацій слід писати на електронну пошту викладача.
Сторінка курсу	https://ami.lnu.edu.ua/course/tekhnichni-kanaly-vytoku-informatsii
Інформація про дисципліну	Дисципліна “Технічні канали витоку інформації” є вибірковою дисципліною з спеціальності 125 – кібербезпека та захист інформації для освітньої програми Кібербезпека, яка викладається у VIII-му семестрі в обсязі 6-х кредитів (за Європейською Кредитно-Трансферною Системою ECTS).
Коротка анотація дисципліни	Курс спрямований на формування у студентів професійних компетентностей та знань про технічні канали витоку інформації, їх впливи на інформацію та засоби її обробки, технічні системи інформації на об'єктах інформаційно-телекомунікаційних мереж.
Мета та цілі дисципліни	Метою курсу є формування у студентів необхідних знань про технічні канали витоку інформації, деструктивні впливи на інформацію та засоби її обробки, технічні заходи та засоби захисту інформації на об’єктах інформаційної діяльності.
Література для вивчення дисципліни	Основна: 1. Богуш В.М., Бровко В.Д., Кобус О.С., В.Д. Козюра В.Д. Технічний захист інформації: теоретичні основи та організаційно-технічне забезпечення. Навч. посіб. – К.: Видавництво Ліра-К, 2023. – 484 с. 2. Богуш В.М., Бровко В.Д., Кобус О.С., В.Д. Козюра В.Д. Технічний захист інформації. Навч. посіб. – К.: Видавництво Ліра-К, 2023. – 508 с. 3. Головін Ю.О., Могилевич Д.І. Основи теорії радіозв'язку – теоретичні основи та практичні аспекти. Навч. посіб. – К.: КПІ ім. Ігоря Сікорського, 2023. – 248 с. https://ela.kpi.ua/server/api/core/bitstreams/93052c4e-fbab-49e5-8dbe-727616651da0/content 4. O'Flynn C., van Woudenberg J. The Hardware Hacking Handbook – Breaking Embedded Security with Hardware Attacks. No Starch Press, US. 2021. – P. 512.

	5. Лаптєв О.А. Виявлення та блокування засобів негласного отримання інформації на об'єктах інформаційної діяльності: навчальний посібник. О.А. Лаптєв, В.А. Савченко, Г.В. Шуклін. – К.: ДУТ, 2020. – 126 с. Додаткова: 6. Long Y., Jiang Q., Yan C., Alam T., Ji X., Xu W., Fu K. EM Eye: Characterizing Electromagnetic Side-channel Eavesdropping on Embedded Cameras. 2024. https://dx.doi.org/10.14722/ndss.2024.24552 7. Paolo Romani IZ1MLL, UT2YR (переклад). SDRsharp, розмалюй чорно-білий етер розмаїттям. 2022. – 186 с. https://airspy.com/downloads/SDRSharp_Big_Book_v5.3_U%D0%90.pdf 8. OSCOR Blue Spectrum Analyzer User Manual. Research Electronics International LLC. Revision 1.2.0.16. – P. 129. https://reiusa.net/wp-content/uploads/2020/12/OSCOR-Blue-Manual-Revision-1.2.0.16.pdf 9. Schalk, G., Bienert R. RFID: MIFARE and Contactless Smartcards in Application. Elektor International Media BV, 2013 – P. 483.
Обсяг курсу	Загальний обсяг: 180 годин. Аудиторних занять: 70 год., з них 28 год. лекцій та 42 год. лабораторних робіт. Самостійної роботи: 110 год.
Очікувані результати навчання	У результаті вивчення навчальної дисципліни студент має набути таких компетентностей: **знати:** • методи технічної розвідки для її запобіганню; • деякі методи пошуку засобів негласного отримання інформації; • фізичні принципи (мікро)електроніки та радіозв'язку в розрізі задач захисту інформації; • апаратні методи впливу на мікроконтролери для подальшого витоку інформації. **вміти:** • ідентифікувати потенційні технічні канали витоку інформації; • здійснювати пошук деяких засобів негласного отримання інформації; • працювати з SDR-приймачами та аналізаторами спектру. **Курс забезпечує набуття таких компетентностей: КІ, КЗ 1, КЗ 2, КЗ 4, КЗ 5, КФ 1-5 та програмних результатів навчання: ПРН 2-31, ПРН 33-40, ПРН 44-53.**
Ключові слова	Аналізатор спектру, вібро-акустичний канал, відеоспостереження, електричний канал, електромагнітний канал, засоби негласного отримання інформації, контроль доступу, мікрофони, небезпечний сигнал, оптичний канал, оптоелектронний канал, параметричний канал, перехоплення, радіохвилі, IQ-сигнал, RFID, SDR-приймач.
Формат курсу	Очний Проведення лекцій, лабораторних робіт і консультацій.
Теми	Теми подані у схемі курсу нижче
Підсумковий контроль, форма	Залік у кінці семестру. Формат заліку: письмовий тестовий.
Пререквізити	Для вивчення курсу студенти потребують базові знання з таких дисциплін: 1) Основи кібербезпеки; 2) Операційні системи та комп'ютерні мережі; 3) Фізичні основи електроніки;

	4) Основи криптографії; 5) Технічні засоби захисту інформації.
Навчальні методи та техніки, які будуть використовуватися під час викладання курсу	Презентації, лекції Демонстрація обладнання Робота з обладнанням Модульний контроль Індивідуальні завдання
Необхідне обладнання	Лабораторія технічних засобів кібербезпеки, обладнана: робочими станціями, з'єднаними в комп'ютерну мережу; демонстраційними системами відеоспостереження, охоронної сигналізації, контролю доступу; спеціальними апаратними та програмними засобами (вимірювальні пристрої, SDR приймачі, тощо).
Критерії оцінювання (окремо для кожного виду навчальної діяльності)	Оцінювання проводиться за 100-бальною шкалою. Бали нараховуються за наступним співвідношенням: • модульний контроль, тестування, усне опитування: 50% семестрової оцінки; максимальна кількість балів 50 • залік: 50% семестрової оцінки; максимальна кількість балів 50 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 незарахування 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. Що таке технічна розвідка? Які засоби вона використовує? 2. Що таке амплітуда та фаза сигналу? Чим відрізняється амплітудна, частотна та фазова маніпуляція? 3. Чи можливо відновити інформацію на HDD? SSD? Як і коли? 4. Чим відрізняється радіозакладка від GSM-закладки? Як їх можна знайти? 5. Чим відрізняється динамічне та діалогове кодування? В чому їх сильні та слабкі сторони? 6. Як здійснюється пошук різних засобів негласного отримання

	інформації? 7. Як зображають сигнал у часовій і частотній областях. Для чого і як використовують аналізатори спектру? 8. У чому різниця між оптичними та оптоелектронними каналами витоку інформації? 9. Що таке спектрограма «водоспад»? Чим SDR-приймач поступається професійному аналізатору спектру? 10. Що таке акустично-електричне перетворення? Як використовується мікрофонний ефект? 11. Що таке ізотропний випромінювач? Яка рекомендована довжина диполь- та штирьової антени? 12. Що таке контрольована зона? Чим відрізняються основні та допоміжні технічні засоби і системи? 13. Що таке квадратурна демодуляція? Які принципи побудови SDR-приймача? 14. Розкажіть про повітряні та вібраційні акустичні канали витоку інформації. 15. Розкажіть про візуальні та оптико-електронні канали витоку інформації. 16. Які електричні канали витоку інформації існують? 17. Що таке IQ-сигнал? Який вигляд діаграми сигнального сузір'я для модуляції 16-QAM? 18. Які стандарти ідентифікаторів RFID ви знаєте? Їх основні властивості та вразливості. 19. Що таке паразитні випромінювання? Наведення? Які джерела їх виникнення? 20. Що таке джерело небезпечного сигналу? Наведіть класифікацію технічних каналів витоку інформації. 21. У чому суть впливу на роботу мікроконтролера шляхом Optical Fault Injection та Electromagnetic Fault Injection? 22. У чому суть впливу на роботу мікроконтролера шляхом Clock Glitching та Voltage Glitching? 23. Які електромагнітні канали витоку інформації існують? 24. Як пов'язані частота та довжина хвилі? Що таке амплітудна, частотна та фазова модуляція?
Опитування	Анкету-оцінку з метою оцінювання якості курсу буде надано по завершенню курсу.

Тиж.	Тема, план, короткі тези	Форма діяльності (заняття)	Література	Завдання, год.	Термін виконання
1	**Тема 1.** Біофізичні механізми мовлення. Акустично-електричне перетворення. Скремблювання звуку. Оцифрування звуку. Диктофони.	лекція, самостійна робота	[1, 2, 5]	2 7	1 тиждень
		лаб.		2	
2	**Тема 2.** Системи радіозв’язку. Фаза, амплітуда, частота та довжина хвилі. Зсув фаз. Класифікація радіохвиль. План розподілу і користування радіочастотним спектром в Україні.	лекція, самостійна робота	[3]	2 7	1 тиждень
		лаб.		4	

3	**Тема 3.** Стандарти технологій радіозв'язку. Класифікація радіоканалів витоку інформації за природою утворення, діапазоном випромінювання, середовищем поширення.	лекція, самостійна робота лаб.	[1, 2, 3]	2 7 2	1 тиждень
4	**Тема 4.** Радіоантени. Діаграма спрямованості. Коефіцієнт підсилення. Смуга пропускання. Розрахунок довжини диполь- та штирьової антени. Сигнал у часовій і частотній областях. Спектрограма «водоспад».	лекція, самостійна робота лаб.	[3, 7, 8]	2 7 4	1 тиждень
5	**Тема 5.** Амплітудна, частотна та фазова модуляція (AM/FM/PM). Амплітудна, частотна та фазова маніпуляція (ASK/FSK/PSK). Радіозакладки. GSM-закладки. Використання рації Quansheng UV-K5.	лекція, самостійна робота лаб.	[3, 5, 7]	2 8 2	1 тиждень
6	**Тема 6.** IQ-сигнал як комплексні числа. Діаграма сигнального сузір'я. Квадратурно-амплітудна модуляція. Мультиплексування. Псевдовипадкове перелаштування робочої частоти.	лекція, самостійна робота лаб.	[3, 7]	2 8 4	1 тиждень
7	**Тема 7.** Принципи побудови SDR-приймача. Квадратурна демодуляція. SDR-приймачі Airspy Mini та RTL-SDR Blog V4. Програма SDR#. Режими NFM/WFM/AM/LSB/USB/ CW/DSB/RAW.	лекція, самостійна робота лаб.	[3, 7]	2 8 2	1 тиждень
8	**Тема 8.** Аналізатори спектру Spectrum Spy та Spektrum. Практичне використання. Функціональні можливості професійного аналізатора спектру OSCOR Blue.	лекція, самостійна робота лаб.	[5, 7, 8]	2 7 4	1 тиждень
9	**Тема 9.** RFID стандартів Em-Marine та MIFARE. Несанкціоноване дублювання. Радіокерування. Динамічне (KeeLoq) та діалогове кодування. Радіоперехоплювачі. ПЗ Universal Radio Hacker. Використання Flipper Zero.	лекція, самостійна робота лаб.	[9]	2 8 2	1 тиждень
10	**Тема 10.** Оптичні канали витоку інформації. Спостережні прилади. Фото- і відеозйомка. Телеоб’єктиви. Приховані камери. Вразливість ЕМ Еуе камер відеоспостереження. Випромінювання в інфрачервоній, видимій та ультрафіолетовій областях спектру. Волоконно-оптичний зв’язок.	лекція, самостійна робота лаб.	[1, 2, 5, 6]	2 7 4	1 тиждень

11	**Тема 11.** Електричні та електромагнітні канали витоку інформації. Паразитні випромінювання. Наведення. Знімання наведених сигналів зі з'єднувальних ліній і сторонніх провідників. Знімання інформаційних сигналів з ліній електроживлення та заземлення. Використання електронних пристроїв перехоплення інформації.	лекція, самостійна робота лаб.	[1, 2, 5]	2 7 2	1 тиждень
12	**Тема 12.** Фізичні принципи збереження інформації – магнітний, оптичний та електронний. Флешпам'ять NOR, NAND, eMMC та UFS. Відновлення даних з HDD. Відновлення даних з SSD та інших пристроїв з флешпам'яттю. Заморожування ОЗП.	лекція, самостійна робота лаб.	[1, 2]	2 7 4	1 тиждень
13	**Тема 13.** Апаратні атаки на мікроконтролери. JTAG. Початковий завантажувач. Clock Glitching. Voltage Glitching. Optical Fault Injection. Electromagnetic Fault Injection.	лекція, самостійна робота лаб.	[4]	2 7 2	1 тиждень
14	**Тема 14.** Огляд історичних і сучасних кейсів витоку інформації технічними каналами. Ендовібратор «Річ» у посольстві США в СРСР, операція «Берлінський туннель» тощо. Задачі технічного захисту інформації та їх важливість.	лекція, самостійна робота лаб.	[1, 2]	2 7 4	1 тиждень