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 засоби захисту 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 засоби захисту 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	Пархуць Любомир Теодорович, д.т.н., професор кафедри кібербезпеки Щербина Микола Юрійович, асистент кафедри кібербезпеки
Контактна інформація викладачів	Liubomyr.Parkhuts@lnu.edu.ua; 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-zasoby-zakhystu-informatsii
Інформація про дисципліну	Дисципліна “Технічні засоби захисту інформації” є нормативною дисципліною з спеціальності 125 – кібербезпека та захист інформації для освітньої програми Кібербезпека, яка викладається у V-му семестрі в обсязі 5-х кредитів (за Європейською Кредитно-Трансферною Системою ECTS).
Коротка анотація дисципліни	Курс спрямований на формування у студентів професійних компетентностей з технічного захисту інформації в сучасних комп'ютерних системах, а також знань про технічні канали витоку інформації, деструктивні впливи на інформацію та засоби її обробки, технічні заходи і засоби захисту інформації на об'єктах інформаційної діяльності.
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	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. Методологія захисту інформації. Аспекти кібербезпеки: підручник. Г.М. Гулак – К.: Видавництво НА СБ України, 2020. – 256 с. 4. 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. 5. Jason Andress. Foundations of Information Security: A Straightforward

	Introduction. No Starch Press, US. 2019. – P. 380.
Обсяг курсу	Загальний обсяг: 150 годин. Аудиторних занять: 64 год., з них 32 год. лекцій та 32 год. лабораторних робіт. Самостійної роботи: 86 год.
Оч33ікувані результати навчання	У результаті вивчення навчальної дисципліни студент має набути таких компетентностей: **знати:** • технічні канали витоку інформації: вібро-акустичний, електричний, електромагнітний, оптичний, оптоелектронний, параметричний; • методи та засоби технічного захисту інформації (пасивні та активні), від витоку зазначеними каналами; • методи пошуку та блокування засобів негласного отримання інформації; • системи відеоспостереження, охоронних сигналізацій, контролю доступу. **вміти:** • організовувати захист інформації від витоку технічними каналами (вібро-акустичним, електричним, електромагнітним, оптичним, оптоелектронним, параметричним); • здійснювати пошук та блокування засобів негласного отримання інформації; • підбирати у відповідності до задач, налаштовувати та використовувати • системи відеоспостереження, охоронних сигналізацій, контролю доступу. **Курс забезпечує набуття таких компетентностей: ІК, КЗ 1, КЗ 2, КЗ 4, КЗ 5, КФ 1-5, КФ 7, КФ 9-12; та програмних результатів навчання: ПРН 2-31, ПРН 33-40, ПРН 44-53.**
Ключові слова	Вібро-акустичний канал, відеоспостереження, електричний канал, електромагнітний канал, засоби негласного отримання інформації, засоби технічного захисту інформації, захист інформації, контроль доступу, методи технічного захисту інформації, оптичний канал, оптоелектронний канал, охоронна сигналізація, параметричний канал.
Формат курсу	Очний Проведення лекцій, лабораторних робіт і консультацій.
Теми	Теми подані у схемі курсу нижче
Підсумковий контроль, форма	Іспит у кінці семестру. Формат іспиту: 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.
Навчальні методи та техніки, які будуть використовуватися під час викладання курсу	Презентації, лекції Демонстрація обладнання Робота з обладнанням Модульний контроль Індивідуальні завдання
Необхідне	Лабораторія технічних засобів кібербезпеки, обладнана: робочими

обладнання	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 • іспит: 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 іспиту	1. Що таке джерело небезпечного сигналу? Наведіть класифікацію технічних каналів витоку інформації. 2. Що таке контрольована зона? Чим відрізняються основні та допоміжні технічні засоби і системи? 3. Що таке технічна розвідка? Які засоби вона використовує? 4. Що таке акустично-електричне перетворення? Як використовується мікрофонний ефект? 5. Розкажіть про повітряні та вібраційні акустичні канали витоку інформації. 6. Розкажіть про параметричні та оптико-електронні канали витоку інформації. 7. Які основні характеристики радіосигналу? Що таке амплітудна, частотна та фазова модуляція? 8. Що таке паразитні випромінювання? Які джерела їх виникнення? Методи захисту? 9. Які електричні канали витоку інформації існують? 10. Які електромагнітні канали витоку інформації існують? 11. У чому різниця між оптичними та оптоелектронними каналами витоку інформації?

	12. Перелічіть організаційні заходи захисту інформації від витоку. 13. У чому різниця між пасивними та активними методами захисту інформації від витоку? 14. Що таке ТЗПІ? Опишіть пасивні технічні заходи захисту інформації від витоку. 15. Що таке ДТЗС? Опишіть активні технічні заходи захисту інформації від витоку. 16. Як здійснюється пошук засобів негласного отримання інформації? 17. Які є способи блокування засобів негласного отримання інформації? 18. У чому різниця між CCD та CMOS сенсорами? Як правильно підібрати кут огляду відеоспостереження? 19. У чому різниця між фіксованими та керованими (PTZ) камерами? З чого складається система IP відеоспостереження? 20. Що таке приймально-контрольна панель? У чому різниця між групами та зонами? Які типи датчиків існують? 21. Які переваги та недоліки дротових і бездротових охоронних систем? Чим відрізняється під'єднання шлейфів NC, EOL/NC та 2EOL/NC? 22. З яких елементів складається СКУД? Що таке iButton? Біометричні ідентифікатори? 23. Які стандарти ідентифікаторів RFID ви знаєте? Їх основні властивості. 24. Як запобігти відновленню інформації на HDD? SSD?
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. Технічні канали витоку інформації** (загальні поняття: інформація з обмеженим доступом (ІзОД); джерело небезпечного сигналу (носія інформації), середовище поширення небезпечного сигналу (носія інформації), засіб технічної розвідки (перехоплення інформації), завади, контрольована зона тощо; основні та допоміжні технічні засоби і системи (ТЗПІ/ДТЗС); класифікація технічних каналів витоку інформації)	лекція, самостійна робота	[1-5]	2 5	1 тиждень
		лаб.	[1-5]	2	
2	**Тема 2. Акустичні канали витоку інформації** (біофізичні механізми мовлення, акустично-електричне перетворення, мікрофонний ефект тощо; відповідні канали витоку – повітряні, електроакустичні, вібраційні, параметричні, оптико-електронні)	лекція, самостійна робота	[1-5]	2 5	1 тиждень
		лаб.	[1-5]	2	
3		лекція, самостійна робота	[1-5]	2 6	1 тиждень
		лаб.	[1-5]	2	
4	**Тема 3. Радіотехнічні канали витоку інформації** (фізичні принципи радіозв'язку, модуляція – амплітудна, частотна та фазова,	лекція, самостійна робота	[1-5]	2 5	1 тиждень
		лаб.	[1-5]	2	

5	паразитні випромінювання тощо; робота з SDR приймачами)	лекція, самостійна робота	[1-5]	2 6	1 тиждень
		лаб.	[1-5]	2	
6	**Тема 4. Електричні канали витоку інформації** (знімання наведених сигналів ПЕМВ ТЗПІ зі з'єднувальних ліній ДТЗС і сторонніх провідників; інформаційних сигналів з ліній електроживлення ТЗПІ; інформаційних сигналів з мереж заземлення ТЗПІ і ДТЗС; інформації шляхом розміщення в ТЗПІ електронних пристроїв перехоплення інформації тощо)	лекція, самостійна робота	[1-5]	2 5	1 тиждень
		лаб.	[1-5]	2	
7	**Тема 5. Електромагнітні канали витоку інформації** (побічні електромагнітні випромінювання (ПЕМВ) елементів ТЗПІ; ПЕМВ на частотах роботи ВЧ генераторів ТЗПІ й ДТЗС; ПЕМВ на частотах самозбудження НЧ підсилювачів ТЗПІ тощо)	лекція, самостійна робота	[1-5]	2 5	1 тиждень
		лаб.	[1-5]	2	
8	**Тема 6. Оптичні канали витоку інформації** (фізичні принципи фотографії, випромінювання в інфрачервоній, видимій та ультрафіолетовій областях спектру, волоконно-оптичний зв'язок тощо)	лекція, самостійна робота	[1-5]	2 5	1 тиждень
		лаб.	[1-5]	2	
9	**Тема 7. Організаційні заходи захисту інформації від витоку** (залучення до робіт організацій з відповідними ліцензіями; категорування й атестація об'єктів ТЗПІ та виділених приміщень; використання на об'єкті сертифікованих ТЗПІ та ДТЗС; встановлення КЗ навколо об'єкта; контроль та обмеження доступу на об'єкти ТЗПІ та у виділені приміщення; введення обмежень у режимах використання технічних засобів, що підлягають захисту; відключення технічних засобів від ліній зв'язку на період проведення секретних заходів тощо)	лекція, самостійна робота	[1-5]	2 6	1 тиждень
		лаб.	[1-5]	2	
10	**Тема 8. Пасивні технічні заходи захисту інформації від витоку** (контроль і обмеження доступу на об'єкти ТЗПІ та у виділені приміщення, локалізація випромінювання, розв'язування інформаційних сигналів тощо)	лекція, самостійна робота	[1-5]	2 5	1 тиждень
		лаб.	[1-5]	2	

11	**Тема 9. Активні технічні заходи захисту інформації від витоку** (просторове зашумлення, лінійне зашумлення, знешкодження підключених до лінії закладних пристроїв за допомогою спеціальних генераторів імпульсів тощо)	лекція, самостійна робота	[1-5]	2 5	1 тиждень
		лаб.	[1-5]	2	
12	**Тема 10. Методи пошуку та блокування засобів негласного отримання інформації** (спеціальне обстеження виділених приміщень; пошук з використанням виявителів пустот, металошукачів і рентгенівських апаратів; пошук з використанням індикаторів електромагнітного поля, радіо частотомірів та інтерцепторів; пристрої приглушення диктофонів, ультразвукового заглушення тощо)	лекція, самостійна робота	[1-5]	2 5	1 тиждень
		лаб.	[1-5]	2	
13	**Тема 11. Системи відеоспостереження** (фізичні принципи: фокусна відстань, діагональ матриці, CCD та CMOS сенсори, роздільна здатність, кут огляду та віддаль до об'єкта, ІЧ підсвітка; фіксовані та керовані (PTZ) камери; аналоговий та цифровий інтерфейси передачі зображення, кодеки MJPEG, MPEG-4 та H.264, багатоканальні відеореєстратори; розпізнавання руху та об'єктів);	лекція, самостійна робота	[1-5]	2 6	1 тиждень
		лаб.	[1-5]	2	
14	**Тема 12. Охоронні сигналізації** (панелі приймально-контрольні; режими охорони; групи та зони; дротові та бездротові системи; під'єднання шлейфів – NC, EOL/NC, 2EOL/NC тощо; типи датчиків – магнітоконтактні, вібрації, руху, розбивання скла, комбіновані, пожежні, затоплення тощо; світло-звукові сирени; комунікація з пультом охорони та користувачем)	лекція, самостійна робота	[1-5]	2 6	1 тиждень
		лаб.	[1-5]	2	
15	**Тема 13. Системи контролю контролю і управління доступом** (автономні (локальні) та	лекція, самостійна робота	[1-5]	2 6	1 тиждень

	централізовані (мережеві) СКУД; перегороджуючі пристрої: електро-защіпки та замки, турнікети, шлюзові кабіни; ідентифікатори та зчитувачі: кодова клавіатура, контактні – iButton, безконтактні – EM-Marine Mifare, NFC, BLE, біометричні – відбитками пальців сітківкою ока, розпізнавання обличчя тощо)	лаб.	[1-5]	2	
16	**Тема 14. Методи відновлення та гарантованого знищення інформації** (фізичні принципи збереження інформації – магнітний, оптичний та електронний; технології відновлення даних на HDD, SSD та інших пристроях з флешпам'яттю; методи знищення інформації в комп'ютерних системах – програмні, механічні та фізичні)	лекція, самостійна робота	[1-5]	2 5	1 тиждень
		лаб.	[1-5]	2	