**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 № 16/23 від 7 вересня 2023 р.)

Завідувач кафедри

 Венгерський П.С.

# Силабус з навчальної дисципліни

# "Комплексні системи 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** | Комплексні системи захисту інформації |
| **Адреса викладання дисципліни** | м. Львів, вул. Університетська 1 |
| **Факультет та кафедра, за якою закріплена дисципліна** | Факультет прикладної математики та інформатики<br>Кафедра кібербезпеки |
| **Галузь знань, шифр та назва спеціальності** | 12 – інформаційні технології<br>125 – кібербезпека та захист інформації |
| **Викладачі дисципліни** | Пархуць Любомир Теодорович, д.т.н., професор кафедри кібербезпеки;<br>Костяк Марина Юріївна, к.т.н., доцент кафедри кібербезпеки |
| **Контактна інформація викладачів** | Liubomyr.Parkhuts@lnu.edu.ua; Maryna.Kostiak@lnu.edu.ua<br>Головний корпус ЛНУ ім. І. Франка, каб. 380.<br>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/academics/bachelor |
| **Інформація про дисципліну** | Дисципліна "Комплексні системи захисту інформації" є нормативною дисципліною зі спеціальності 125 – кібербезпека та захист інформації для освітньої програми Кібербезпека, яка викладається в 5,6 семестрах в обсязі 6 кредитів (за Європейською Кредитно-Трансферною Системою ECTS). |
| **Коротка анотація дисципліни** | Навчальна дисципліна "Комплексні системи захисту інформації" в системі підготовки фахівців освітньо-кваліфікаційного рівня бакалавр є загальноосвітнім курсом технічного спрямування. Предметом вивчення навчальної дисципліни є: вивчення сучасних методів проектування систем захисту інформації; сукупність основних теоретичних положень створення комплексних систем захисту інформації; процесів забезпечення необхідного рівня захищеності інформації; особливості технологій проектування та забезпечення захисту інформації з обмеженим доступом на об’єктах . |
| **Мета та цілі дисципліни** | Метою курсу нормативної дисципліни є опанування навичками та основними принципами розробки комплексних систем захисту інформації з обмеженим доступом на об'єкті. |
| **Література для вивчення дисципліни** | *Основна література*<br>1. В.Д. Козюра, В.О. Хорошко, М.Є. Шелест, Ю.М. Ткач, Я.Ю. Усов Комплексні системи захисту інформації в інформаційнотелекомунікаційних системах. – Н.: ТПК «Орхідея», - 2019. – 144с.<br>2. 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.<br>3. Закон України «Про телекомунікації» (Відомості Верховної Ради України ВВР, №12, ст..155).<br>4. Закон України „Про захист інформації в |

| | |
|---|---|
| | інформаційнотелекомунікаційних системах” (Відомості Верховної Ради України (ВВР), N 31, ст.286).<br>*Додаткова література*<br>5. Закон України "Про державну таємницю": Закон України від 21.09.99 № 1079-XIV // Відомості Верховної Ради України. – 1999. – № 49. – Ст. 428.<br>6. Про інформацію: Закон України від 02.10.92 № 2657-XII // Відомості Верховної Ради України. – 1992. – № 48. – Ст. 650.<br>7. Антонюк А.О. Основи захисту інформації в автоматизованих системах / А. О. Антонюк. – К.: КМ Академія, – 2016. – 244 с.<br>8. ДСТУ 3396.0-96. Захист інформації. Технічний захист інформації. Основні положення.<br>9. ДСТУ 3396.1-96. Захист інформації. Технічний захист інформації. Порядок проведення робіт.<br>10. НД ТЗІ 1.1.-002-99. Загальні положення захисту інформації в комп’ютерних системах від несанкціонованого доступу.<br>11. НД ТЗІ 2.5.-004-99. Критерії оцінки захищеності інформації в комп`ютерних системах від несанкціонованого доступу.<br>12. НД ТЗІ 2.5.-005-99. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу.<br>13. НД ТЗІ 3.7.-001-99. Методичні вказівки щодо розроблення технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі.<br>14. Порядок проведення робіт із сертифікації засобів забезпечення технічного захисту інформації загального призначення.<br>15. НД ТЗІ 1.4.-001-2000. Типове положення про службу захисту в автоматизованій системі.<br>16. Тимчасове положення про категоріювання об’єктів (ТПКО – 95).<br>17. НД ТЗІ 2.7.- 001-99. Технічний захист інформації на програмно-керованих АТС загального користування. Порядок виконання робіт.<br>18. НД ТЗІ 3.6.-001-2000. Технічний захист інформації. Комп’ютерні системи. Порядок створення, впровадження, супроводження та модернізації засобів механічного захисту інформації від несанкціонованого доступу.<br>19. НД ТЗІ 3.7.-002-99. Технічний захист інформації на програмно-керованих АТС загального користування. Методика оцінки захищеності інформації (базова).<br>20. НД ТЗІ 4.7.- 002-2001. Визначення захищеності мовної інформації від витоку акустичним і віброакустичним каналами. Методичні вказівки.<br>21. http://dstszi.kmu.gov.ua/dstszi/control/uk/publish/article?art_id=89740&cat_id=89734<br>22. НД ТЗІ 1.1-005-07. Захист інформації на об’єктах інформаційної діяльності. Створення комплексу ТЗІ. Основні положення. ДССЗЗІ України. – Київ. – 2007.<br>23. НД ТЗІ 1.6-003-04 Створення комплексів технічного захисту інформації на об’єктах інформаційної діяльності. Правила розроблення, побудови, викладення та оформлення моделі загроз для інформації. ДССЗЗІ України. – Київ. – 2004.<br>24. НД ТЗІ 3.1-001-07. Захист інформації на об’єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Передпроектні роботи. ДССЗЗІ України. – Київ. – 2007.<br>25. НД ТЗІ 3.3-001-07. Захист інформації на об’єктах інформаційної |

| | |
|---|---|
| | діяльності. Створення комплексу технічного захисту інформації. Порядок розроблення та впровадження заходів із захисту інформації. ДССЗЗІ України. – Київ. – 2007.<br>26. НД ТЗІ 2.1-002-07. Захист інформації на об'єктах інформаційної діяльності. Випробування комплексу ТЗІ. Основні положення. ДССЗЗІ України. – Київ. – 2007.<br>27. Захист засобів і каналів телефонного зв'язку / В.Б.Дудикевич, В.В.Хома, Л.Т.Пархуць // Навчальний посібник з грифом МОН України. – Львів: Видав. Львівської політехніки. – 2012. – 212 с. |
| **Обсяг курсу** | Загальний обсяг: 180 годин. Аудиторних занять: 112 год., з них 48 год. лекцій та 64год. лабораторних робіт. Самостійної роботи: 68 год. |
| **Очікувані результати навчання** | У результаті вивчення навчальної дисципліни студент має набути таких компетентностей:<br>**<u>знати:</u>**<br>– основні форми представлення інформації;<br>– проблеми захисту даних;<br>– сигнали поширення та передачі інформації;<br>– основі джерела та шляхи витоку інформації;<br>– способи несанкціонованого перехоплення інформації;<br>– основні технічні засоби, що використовуються для несанкціонованого перехоплення інформації;<br>– методи та засоби захисту інформації;<br>– основні технічні засоби, що використовуються для захисту інформації від несанкціонованого перехоплення;<br>– нормативно-правові документи щодо створення комплексних систем захисту інформації;<br>– порядок створення комплексних систем інформації.<br>**<u>вміти:</u>**<br>– аналізувати приміщення щодо можливих джерел та шляхів витоку інформації;<br>– аналізувати результати обстеження об'єкту захисту щодо наявності інформації з обмеженим доступом;<br>– виявляти та аналізувати можливі технічні канали витоку інформації та будувати модель загроз;<br>– проектувати комплексну систему захисту інформації згідно нормативних вимог;<br>– виконувати захист приміщень від несанкціонованого перехоплення інформації;<br>**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-16, ПРН-18, ПРН-21, ПРН-23, ПРН-26, ПРН-31, ПРН-34, ПРН-36. ПРН-38, ПРН-39. |
| **Ключові слова** | Захист інформації, загроза, вразливість, конфіденційність, цілісність, технічні канали витоку інформації, пасивні методи захисту інформації, активні методи захисту інформації, комплексна система захисту інформації. |
| **Формат курсу** | Очний. Проведення лекцій, практичних робіт і консультацій. |
| **Підсумковий контроль, форма** | Іспит у кінці 6 семестру |
| **Навчальні методи та техніки, які** | Презентації, лекції.<br>Модульний контроль.<br>Практичні роботи. |

| | |
|---|---|
| **будуть використовуватися під час викладання курсу** | Індивідуальні завдання на створення КСЗІ. |
| **Необхідне обладнання** | Комп'ютери чи ноутбуки із встановленою операційною системою Windows; мультимедійний проектор; доступ до мережі Інтернет; програмне забезпечення (зокрема Microsoft Office: Word, Excel, Visio, PowerPoint)/ |
| **Критерії оцінювання (окремо для кожного виду навчальної діяльності)** | Оцінювання проводиться за 100-бальною шкалою. Бали нараховуються за наступним співвідношенням:<br>• модульний контроль, тестування, усне опитування: 50% семестрової оцінки; максимальна кількість балів 50;<br>• залік (у вигляді тесту): 50% семестрової оцінки; максимальна кількість балів 50;<br>Підсумкова максимальна кількість балів 100.<br>**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.<br>**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.<br>**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.<br>**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.<br>Жодні форми порушення академічної доброчесності не толеруються. |
| Питання до екзамену. | 1. Основні напрямки захисту інформації з обмеженим доступом.<br>2. Основні форми представлення інформації.<br>3. Основні об’єкти захисту інформації.<br>4. Технічні засоби прийому, обробки, збереження і передачі інформації.<br>5. Допоміжні технічні засоби і системи.<br>6. Об’єкт ТЗПІ. Поняття небезпечних зон. Випадкові антени.<br>7. Класифікація і характеристика технічних каналів витоку інформації.<br>8. Електромагнітні, електричні і параметричні канали витоку інформації.<br>9. Повітряні, вібраційні, електроакустичні, оптико-електронні канали.<br>10. Проектно-архітектурні рішення щодо захисту інформації.<br>11. Проведення організаційних заходів. |

| | |
|---|---|
| | 12. Пасивні заходи захисту інформації (контроль і обмеження доступу на об’єкти ТЗПІ, локалізація випромінювань, розв’язка інформаційних сигналів)<br>13. Активні заходи захисту інформації (просторове зашумлення, лінійне зашумлення, знищення закладних пристроїв) технічні заходи<br>14. Виявлення портативних електронних пристроїв перехоплення інформації (закладних пристроїв): спеціальні обстеження, спеціальна перевірка.<br>15. Побічне електромагнітне випромінювання.<br>16. Екранування технічних засобів. Електростатичне екранування. Магнітостатичне екранування. Електромагнітне екранування. Схеми та вимоги до матеріалів екранування.<br>17. Заземлення технічних засобів. Основні вимоги до системи заземлення.<br>18. Опір заземлення. Питомий опір грунтів. Вплив кліматичних умов.<br>19. Матеріали для виконання заземлення. Виконання заземлення та захист від пошкоджень.<br>20. Фільтрація інформаційних сигналів. Роздільні трансформатори.<br>21. Завадопоглинаючі фільтри. Основні вимоги до захисних фільтрів. Конструктивне виконання та характеристики фільтрів.<br>22. Просторове і лінійне зашумлення. Основні вимоги до системи просторового зашумлення.<br>23. Системи "білий шум" та "синфазні завади". Генератори шуму, типи та основні характеристики. Ефективність просторового зашумлення.<br>24. Системи лінійного зашумлення та їх застосування.<br>25. Пасивні та активні методи і засоби захисту інформації.<br>26. Звукоізоляція приміщень. Основні вимоги та оцінка ефективності звукоізоляції.<br>27. Звукоізоляція дверей та вікон приміщення. Використання акустичних екранів. Матеріали, що використовуються для звукоізоляції.<br>28. Звуковбирні властивості матеріалів та показники їх ефективності. Використання спеціальних кабін.<br>29. Акустичне маскування. Віброакустичне маскування.<br>30. Генератори акустичного шуму. Структура та основні характеристики систем активного віброакустичного маскування. Дотримання вимог охорони праці при використання активних засобів акустичного маскування приміщень.<br>31. Виявлення і придушення диктофонів і акустичних закладок. Детектори диктофонів.<br>32. Пристрої електромагнітного придушення диктофонів. Системи ультразвукового придушення диктофонів. Постійний радіоконтроль приміщень.<br>33. Встановлення прицільних радіозавад. Системи просторового електромагнітного зашумлення.<br>34. Фільтрація сигналів. Розділові трансформатори та завадопоглинаючі фільтри.<br>35. Особливості та шляхи перехоплення інформації з використанням телефонних ліній.<br>36. Пасивні та активні методи захисту.<br>37. Обмеження інформативних сигналів.<br>38. Фільтрація інформативних сигналів. Відключення джерел інформативних сигналів.<br>39. Лінійне зашумлення телефонних ліній.<br>40. Метод синфазної маскуючої НЧ завади. Метод ВЧ маскуючої завади. |

| | |
|---|---|
| | 41. Метод ультразвукової маскуючої завади. Метод підвищення напруги.<br>42. Метод "обнулення". Компенсаційний метод. Метод "випалювання".<br>43. Приклади технічної реалізації засобів для захисту телефонних ліній та їх характеристики.<br>44. Порядок створення комплексної системи захисту інформації (КСЗІ).<br>45. Основні етапи створення КСЗІ.<br>46. Порядок проведення обстеження об'єкту захисту.<br>47. Формування політики безпеки об'єкту захисту.<br>48. Створення технічного завдання на побудову КСЗІ<br>49. Введення в дію та експлуатація створеної КСЗІ. |
| **Опитування** | Анкету-оцінку з метою оцінювання якості курсу буде надано після завершенню курсу. |

## Схема курсу

## Лекційні заняття

| № | Назви тем лекційних занять | Год. |
|---|---|---|
| 1. | **Вступ.**<br>Предмет дисципліни та її завдання. Зв'язок з іншими дисциплінами спеціальності. Важливість проблеми та необхідність створення комплексної систем захисту інформації.<br>**Тема 1. Обґрунтування необхідності створення КСЗІ**<br>Підстави для визначення необхідності створення КСЗІ. Норми та вимоги чинного законодавства, які встановлюють обов'язковість обмеження доступу до певних видів інформації або забезпечення її цілісності чи доступності. Вихідні дані для обґрунтування необхідності створення КСЗІ: аналіз нормативно-правових актів; визначення наявності у складі інформації, яка потребує обмеження доступу до неї; оцінка можливих переваг (фінансово-економічних, соціальних і т.п.) створення КСЗІ. Прийняття рішення про необхідність створення КСЗІ. | 4 |
| 2. | **Тема 2. Аналіз об'єкту функціонування КСЗІ**<br>Аналіз та детальне обстеження об'єкту функціонування КСЗІ. Підготовка вихідних даних для формування вимог до КСЗІ. Опис середовища функціонування КСЗІ. Документування результатів обстеження. Розробка концепції КСЗІ (основні принципи і підходи побудови), визначення основних завдань і характеристик, функціональних комплексів та варіантів їх реалізації. Обстеження, аналіз та опис об'єкту КСЗІ. Загальна структурна схема об'єкту захисту, види і характеристики каналів зв'язку. Оформлення акту результатів обстеження. Затвердження переліку об'єктів захисту. Визначення потенційних загроз для інформації і розроблення моделі загроз та моделі порушника. Побудова плану захисту об'єкту. | 4 |
| 3. | **Тема 3. Аналіз результатів обстеження, ризиків та оформлення звіту про обстеження об'єкту захисту**<br>Визначення завдання захисту інформації на об'єкті. Вирішення задач та основних напрямів забезпечення захисту. Організаційні, інженерно-технічні, технічні, криптографічні та інші заходи захисту інформації КСЗІ. Оформлення звіту про виконання робіт та заявки на розробку КСЗІ. | 4 |
| 4. | **Тема 4. Створення та аналіз моделі загроз на об'єкті захисту.** | 4 |

| № | Назви тем лекційних занять | Год. |
|---|---|---|
| | Аналіз ризиків, визначення переліку можливих загроз. Прогнозування загальної структури та складу КСЗІ, можливих заходів, методів та засобів захисту інформації, допустимих обмежень щодо застосування певних заходів і засобів захисту. | |
| 5. | **Тема 5. Розробка політики безпеки інформації в КСЗІ**<br>Уточнення моделі загроз та можливих порушників, можливих ризиків. Проведення додаткових досліджень для пошуку шляхів реалізації завдання на створення КСЗІ. Оформлення і затвердження політики безпеки. Альтернативні варіанти концепції створення КСЗІ і планів їх реалізації. Оцінка переваг і недоліків кожного варіанту, вибір оптимального варіанту. Оформлення концепції у вигляді звіту. Вибір основних рішень з протидії всім суттєвим загрозам. Формування загальних вимог, правил, обмежень, рекомендацій, заходів і засобів захисту інформації. Документальне оформлення політики безпеки інформації. | 6 |
| 6. | **Тема 6. Технічне завдання на створення КСЗІ**<br>Початкові вихідні дані для розроблення технічного завдання (ТЗ) на КСЗІ. Функціональний профіль захищеності від несанкціонованого доступу і вимоги до захищеності інформації від витоку технічними каналами. Вимоги до захищеності інформації від витоку технічними каналами. Вибір функціонального профілю захищеності і вимог до показників захищеності інформації від витоку технічними каналами. Перелік основних робіт етапу формування ТЗ. Класифікація та опис ресурсів об’єкту. Визначення переліку загроз і можливих каналів витоку інформації. Визначення вимог до організаційних, фізичних та інших заходів захисту. Прийняття остаточного рішення про склад КСЗІ. | 4 |
| 7. | **Тема 7. Зміст та основні розділи технічного завдання на КСЗІ**<br>Загальні відомості. Мета і призначення системи захисту інформації. Загальна характеристика системи та умов її функціонування. Вимоги до системи захисту інформації. Вимоги до складу проектної та експлуатаційної документації. Етапи виконання робіт. Порядок внесення змін і доповнень до ТЗ. Порядок проведення випробувань системи захисту інформації. Вимоги до змісту розділів технічного завдання. Загальні відомості. Перелік документів, на підставі яких створюється КСЗІ. Планові терміни початку і закінчення роботи із створення КСЗІ. Порядок оформлення і подання замовнику результатів робіт із створення КСЗІ. | 6 |
| 8. | **Тема 8. Визначення мети і призначення системи захисту інформації**<br>Нормативно-правові акти та нормативні документи, що регламентують порядок захисту інформації в АС. Функціональне призначення і особливості застосування. Загальна структурна схема і склад об’єкту. Технічні характеристики каналів зв'язку. Характеристики інформації, що обробляється. Характеристики фізичного середовища. Загальна технічна характеристика КСЗІ. Особливості реалізованих організаційних, фізичних та інших заходів захисту. Потенційні загрози інформації. | 4 |
| 9. | **Тема 9. Формулювання основних вимог до системи захисту інформації**<br>Формулювання вимог до системи захисту інформації в частині захисту від НСД. Функціональний профіль захищеності. Вимоги до послуг безпеки: онфіденційність; цілісність; доступність; спостереженість. Вимоги до КСЗІ в частині захисту від витоку інформації технічними каналами. Загальні вимоги до об'єктів, що захищаються. Визначення засобів захисту і засобів їх використання. Перелік | 6 |

| № | Назви тем лекційних занять | Год. |
|---|---|---|
| | нормативних і методичних документів щодо захисту інформації від витоку технічними каналами. | |
| 10. | **Тема 10. Етапи виконання робіт та порядок проведення випробувань**<br>Попереднє проектування і розробки КСЗІ. Складання календарного плану. Терміни проведення робіт за окремими етапами, види звітності і форми подання результатів замовнику. Порядок внесення змін і доповнень до технічного завдання на створення КСЗІ. Доповнення до ТЗ на створення КСЗІ. Розробка комплексної системи захисту інформації. Вимоги до звітної документації. Оформлення остаточного звіту про КСЗІ. | 4 |
| 11. | **Підсумкове заняття** | 2 |
| **Усього годин** | | **48** |

**Практичні заняття**

| № | Назви тем занять | Год. |
|---|---|---|
| 1. | Обстеження об'єкту захисту. | 8 |
| 2. | Детальний аналіз результатів обстеження об’єкту. | 8 |
| 3. | Попередній вибір варіанту побудови КСЗІ. | 8 |
| 4. | Розроблення завдання на створення КСЗІ. | 8 |
| 5. | Формування політики безпеки на об'єкті захисту. | 4 |
| 6. | Формування вимог до комплексної системи захисту інформації. | 4 |
| 7. | Приклади розроблення технічного завдання на КСЗІ. | 6 |
| 8. | Зміст та наповнення технічного завдання. | 6 |
| 9. | Етапи створення КСЗІ. | 6 |
| 10. | Оформлення завершального звіту про створену КСЗІ. | 6 |
| **Усього годин** | | **64** |