МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Волинський національний університет імені Лесі Українки

Факультет інформаційних технологій і математики

СИЛАБУС

«Комплексна система захисту інформації»

нормативної навчальної дисципліни

підготовки бакалавра з кібербезпеки

галузь знань 12 Інформаційні технології

спеціальність 125 Кібербезпека та захист інформації

освітньо-професійна програма Кібербезпека та захист інформації

Луцьк – 2023

Силабус навчальної дисципліни «Комплексні системи захисту інформації» підготовки бакалавра, галузі знань 12 Інформаційні технології спеціальності Кібербезпека та захист інформації за освітньо-професійною програмою Кібербезпека та захист інформації.

Розробник: Лаптєв О. А., професор кафедри комп'ютерних наук та кібербезпеки, доктор технічних наук, старший науковий співробітник,

Погоджено
Гарант освітньо-професійної програми:

Глинчук Л.Я.

Силабус освітнього компонента затверджено на засіданні кафедри комп'ютерних наук та кібербезпеки

протокол № 2 від 28 вересня 2023 р.

Завідувач кафедри:  Гришанович Т. О.

1.Опис навчальної дисципліни

Таблиця 1

<table>
<tr><th>Найменування показників</th><th>Галузь знань, спеціальність, освітньо-професійна програма, освітній рівень</th><th>Характеристика навчальної дисципліни</th></tr>
<tr><td>Денна форма навчання</td><td rowspan="8">12 Інформаційні технології

125 Кібербезпека та захист інформації

Кібербезпека та захист інформації</td><td>Нормативна</td></tr>
<tr><td rowspan="6">Кількість годин/кредитів 120/4</td><td>Рік навчання <u>4</u></td></tr>
<tr><td>Семестр_7-ий</td></tr>
<tr><td>Години:<u>150</u></td></tr>
<tr><td>Кредити: <u>5</u></td></tr>
<tr><td>Лекцій: <u>56 год.</u></td></tr>
<tr><td>Лабораторні роботи : <u>70год.</u></td></tr>
<tr><td rowspan="3">ІНДЗ: немає</td><td>Самостійна робота <u>14 год.</u></td></tr>
<tr><td>Консультації: <u>10 год.</u></td></tr>
<tr><td>Форма контролю: <u>екзамен</u></td></tr>
<tr><td>Мова навчання</td><td>українська</td></tr>
</table>

II. Інформація про викладача

ПІП: Лаптєв Олександр Анатолійович
Науковий ступінь: доктор технічних наук
Вчене звання: старший науковий співробітник
Посада: професор кафедри комп’ютерних наук та кібербезпеки
Контактна інформація (номер мобільного зв’язку, електронна адреса): +380674348001, Alaptev64@ukr.net
Дні занять (посилання на електронний розклад):
https://us04web.zoom.us/j/7639442912?pwd=GQ7a6Mq99IamC2mMAMzzh8EF016gEj.1

III. Опис дисципліни

1. **Анотація курсу:**

Навчальна задача дисципліни «Комплексні системи захисту інформації» полягає у підвищенні рівня знань здобувачів з теорії і практики захисту інформації технічними засобами, набуття вмінь і навичок з виявлення технічних каналів витоку інформації, їх блокування, створенні та впровадженні комплексів технічного захисту інформації, в знанні основ організації та порядку виконання робіт із створення комплексних систем захисту інформації телекомунікаційних систем залежно від характеру об'єкта захисту.

2. Пререквізити/постреквізити

Пререквізити: Базові знання інформаційних технологій та захисту інформації

Постреквізити: Знання та вміння є базовими для вивчення наступних навчальних дисциплін.

3. Мета дисципліни – сформувати у здобувачів теоретичних знань та практичних навичок самостійної роботи з забезпечення комплексного захисту інформації на об'єктах інформаційної діяльності на основі нормативно-правових документів, національних та міжнародних стандартів. Дати здобувачам поглиблені знання в опануванні загальних теоретичних знань та практичних навичок щодо розробки типової стратегії і організації комплексної системи захисту інформації. Вивчення особливостей побудови комплексних систем захисту інформації та централізованого управління системою інформаційної безпеки.

4. Результати навчання (компетентності).

Знання теоретичних основ та вміння свідомого поводження з інформацією в умовах використання сучасних інформаційно-комунікаційних засобів та враховування отриманих знань у практичної діяльності за обраної спеціальності.

Інтегральна компетентність: Здатність розв'язувати складні спеціалізовані задачі та практичні проблеми у сфері захисту інформації та кібербезпеки.

Загальні компетенції:

ЗК 1. Здатність застосовувати знання у практичних ситуаціях.
ЗК 2. Знання та розуміння предметної області та розуміння професії.
ЗК 4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням.
ЗК 5. Здатність до пошуку, оброблення та аналізу інформації.

Спеціальні компетенції:

ФК 7. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.).
ФК 9. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною безпекою та/або кібербезпекою.

Володіти елементарними навичками програмування, навичками використання математичних методів в інформаційних системах та роботи в мережі, дискретної математики, електротехніки та електроніки, теорії алгоритмів.

4. Завдання (навчальні цілі) навчальної дисципліни– забезпечення стабільних базових теоретичних знань, теорії і практики щодо управління інформаційною та кібернетичною безпекою на основі існуючих технологій та програмних продуктів**.**

Сприяти ефективному формуванню у здобувачів наступних професійних компетентностей:

ПРН 1. Застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації.
ПРН 3. Використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності.
ПРН 7. Діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та/або кібербезпеки.
ПРН 15. Використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій.
ПРН 18. Використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів.

ПРН 19. Застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах.
ПРН 21. Вирішувати задачі забезпечення та супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління доступом згідно встановленої політики безпеки в інформаційних та інформаційно- телекомунікаційних (автоматизованих) системах.
ПРН 30. Здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно-телекомунікаційних систем.
ПРН 31. Застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем.
ПРН 35. Вирішувати задачі забезпечення та супроводу комплексних систем захисту інформації, а також протидії несанкціонованому доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно- телекомунікаційних (автоматизованих) системах згідно встановленої політики інформаційної і\або кібербезпеки.
ПРН 36. Виявляти небезпечні сигнали технічних засобів.
ПРН 42. Впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки.
ПРН 50. Забезпечувати функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних).
ПРН 51. Підтримувати працездатність та забезпечувати конфігурування систем виявлення вторгнень в інформаційно-телекомунікаційних системах.
ПРН 52. Використовувати інструментарій для моніторингу процесів в інформаційно-телекомунікаційних системах.
ПРН 53. Вирішувати задачі аналізу програмного коду на наявність можливих загроз.

5. Структура навчальної дисципліни

№ п/п	Назва теми*	Кількість годин			
		Лекції	**П.р.**	**Л.р.**	**С. р.**
Змістовий модуль 1 "Нормативно-правові акти комплексної системи захисту інформації"					
1	Тема 1. Загальні положення та вимоги в частині організації робіт із захисту інформації.	2		-	
2	Тема 2. Правові підстави та основні положення щодо створення КСЗІ та комплексу ТЗІ в Україні	2		4	
3	Тема 3. Основні положення про службу захисту інформації. Технічний захист інформації.	6		6	2
4	Тема 4. Захист інформації в АС від НСД.	6		6	
5	Тема 5.Захист інформації в АС від витоку технічними каналами	2		6	2
6	Тема 6. Захист інформації в АС від руйнування каналами спеціального впливу.	4		6	
7	Тема 7. Порядок проведення робіт зі створення КСЗІ.	6		6	2
	Всього за МК-1	**28**		**34**	**6**
Змістовий модуль 2 "Побудова системи і основних підсистем КСЗІ					
8	Тема 8. Технічне завдання на створення КСЗІ в АС.	6		6	
9	Тема 9. Основи захисту інформації в ІС.	6		6	2
10	Тема 10. Особливості проектування КСЗІ для АС різних класів. Оцінка ефективності та оптимізація КСЗІ.	6		-	2
11	Тема 11. Перспективні напрями розвитку комплексу ЗІ в	2		8	2

	розподілених обчислювальних середовищах (РОС).				
12	Тема 12. Випробування комплексу технічного захисту інформації та його атестація.	2		8	2
13	Тема 13. Введення КСЗІ в дію.	6		8	
	Всього за МК-2	**28**		**36**	**8**
	Консультація		**10**		
	Всього за навчальною дисципліною	**56**		**70**	**14**

Загальний обсяг **150** *год.,* в тому числі:
Лекцій **– 56** *год.*
Лабораторні – **70** *год*
Консультації**– 10** *год*
Самостійна робота **– 14** *год.*

8. Питання до екзамену

1. Назвіть методи підвищення енергетичної та структурної таємності системи передавання інформації.
2. Дайте визначення поняття комплексного захисту інформації
3. Які вам відомі підходи до класифікації загроз безпеці інформації?
4. Порівняйте їх між собою з огляду найбільшої відповідності практичним потребам створення систем захисту інформації.
5. Охарактеризуйте основні принципи системної класифікації загроз безпеці інформації.
6. Наведіть класифікаційну структуру каналів несанкціонованого отримання інформації.
7. Дайте визначення поняттю "Технічний канал витоку інформації". Назвіть основні види технічних каналів.
8. Дайте класифікацію джерел витоку інформації.
9. Наведіть відомі вам методи і засоби контролю акустичної інформації.
10. Розкрийте зміст методів контролю інформації технічними засобами в каналах телефонного зв'язку.
11. Назвіть методи контролю інформації, що обробляється засобами обчислювальної техніки.
12. Охарактеризуйте основні способи запобігання витоку інформації по технічних каналах. Охарактеризуйте способи захисту інформації в каналах зв'язку.
13. Сформулюйте основні концептуальні положення теорії захисту інформації.
14. Розкрийте зміст функції захисту інформації. Які з функцій утворюють повну множину функцій захисту?
15. Сформулюйте завдання захисту і назвіть десять класів завдань, що створюють репрезентативну множину задач захисту.
16. Приведіть класифікацію засобів захисту інформації. Які переваги і недоліки програмних, апаратних та організаційних засобів захисту інформації?
17. Як впливають показники інформації, що захищається, на структуру і підходи до проектування системи захисту інформації?
18. Розкрийте зміст короткострокового, середньострокового і довгострокового управління процесами захисту інформації.
19. Сформулюйте основні вимоги до системи нормативно-правових документів, що регламентують процеси комплексного захисту інформації.
20. Сформулювати задачу оптимального вибору методів захисту для кожного конкретного об’єкта і для системи в цілому.
21. Розкрити критерій вибору засобів і методів захисту.
22. Розкрити задачу мінімізації вартості та ефективності забезпечення систем захисту об’єкта.
23. Розкрити задачу мінімізації вірогідності злому усіх методів, які використовуються для захисту об’єкта.
24. Розкрити задачу мінімізації втрат від злому усіх механізмів захисту (методів захисту), які використовуються для захисту об’єкта.
25. Розкрити та пояснити заходи, які виконуються при створенні КСЗІ.
26. Програмні закладки та їх складові. Класифікація програмних закладок.
27. Які основні характеристики телекомунікаційної системи як об'єкта захисту.
28. Розкрийте поняття загрози інформаційної безпеки. Які основні напрями захисту інформації?
29. Класифікація загроз інформаційної безпеки за компонентами інформаційних систем, на які вони націлені.
30. Класифікація загроз інформаційної безпеки за характером впливу
31. Класифікація загроз інформаційної безпеки за розміщенням їх джерела. Які основні види загроз безпеки інформаційним технологіям?
32. Основні техногенні передбачувані та непередбачені загрози інформаційній системи

33. Яку систему складають дестабілізуючі чинники відповідно до технології і функціонування інформації?

34. Привести структуру каналу витоку інформації та дати характеристику середовищу передачі інформації.

35. Якими видами можуть бути представлені природні канали витоку ?

36. Дайте характеристику каналам витоку інформації, які створені закладними пристроями? Які основні тенденції та шляхи розвитку закладних пистроїв?

37. Які основні методи захисту від витоку інформації з обмеженим доступом шляхом прослуховування?

38. Як залежно від типу створюваного електромагнітного поля розрізняють види екранування?

39. Які методи забезпечують зниження потужності випромінювань і наведень?

40. Які основні методи захисту інформації від НСД в автоматизованих системах?

41. Дайте характеристику основним та допоміжним технічним засобам та системам.

42. Розкрийте поняття зони 1, зони 2 та контрольованої зони.

43. Як класифікуються ТКВІ за фізичними ефектами, процесами? Як класифікуються ТКВІ за носієм, що утворюється джерелом небезпечного сигналу?

44. Як класифікуються ТКВІ за способом перехоплення інформації засобами розвідки противника?

45. Дайте характеристику технічним каналам витоку інформації через допоміжні технічні засоби і системи та сторонні провідники.

46. Дайте характеристику електричним каналам витоку інформації, які виникають в результаті просочування небезпечних сигналів в ланцюги електроживлення.

47. Дайте характеристику електричним каналам витоку інформації, які виникають в результаті просочування небезпечних сигналів в ланцюги заземлення.

48. Дайте характеристику параметричним каналам витоку інформації, що обробляється в основних технічних засобах і системах.

49. Дайте характеристику акустичним та акустовібраційним каналам витоку мовної інформації.

50. Дайте характеристику акустоелектричним та акустооптичним каналам витоку мовної інформації.

51. Дайте характеристику параметричним каналам витоку мовної інформації.

52. Умови обробки інформації в системі.

53. Критерії оцінки захищеності інформації в АС від НСД. КВ-4.

54. Яка інформація в захищеній системі підлягає обов'язковій реєстрації.

55. Критерії оцінки захищеності інформації в АС від НСД. ЦД-1.

56. Що таке АС класу «1», «2», «3».

57. Критерії оцінки захищеності інформації в АС від НСД. ЦД-2.

58. Порядок розроблення та оформлення програм і методик випробувань Що наводять у розділі “Вимоги щодо забезпечення охорони державної таємниці».

59. Критерії оцінки захищеності інформації в АС від НСД. ЦД-3.

60. Атестація комплексів ТЗІ.

61. Основні етапи атестації комплексу ТЗІ.

62. Критерії оцінки захищеності інформації в АС від НСД. ЦД-4.

63. Зміст другого етапу створення комплексу ТЗІ “Розроблення та впровадження заходів із захисту інформації” на ОІД.

64. Завдання Служби захисту інформації.

9. Політика оцінювання

Здобувач має виконати у повному обсязі усі види діяльності із навчальної дисципліни «Нормативно-правове забезпечення інформаційної безпеки», бути присутніми на аудиторних

заняттях. Якщо здобувач відсутній на занятті, він може надіслати виконане семінарське заняття у письмовому вигляді. Претендувати на максимальну кількість балів можна, якщо семінарське виконане у вигляді презентацій, використані нові актуальні наукові джерела, робота є авторською, без порушень авторських прав.

Освітній процес відповідає «Положенню про поточне та підсумкове оцінювання знань студентів Волинського національного університету імені Лесі Українки» від 11 вересня 2020 р. (https://bit.ly/39In2ac). Іспит виставляється автоматично за умови, якщо студент виконав усі види навчальної роботи та отримав не менше ніж 75 балів зі 100 можливих.

Вирішення спірних питань у галузі академічної доброчесності здійснюється на підставі Положення про систему запобігання та виявлення академічного плагіату у науково-дослідній діяльності здобувачів вищої освіти і науково-педагогічних працівників Східноєвропейського національного університету імені Лесі Українки (від 10 лютого 2017 р.) (https://bit.ly/3lNJD7N).

Конфліктні ситуації вирішуються згідно Положення про порядок і процедури вирішення конфліктних ситуацій у Волинському національному університеті імені Лесі Українки (https://bit.ly/33MTIM).

Згідно Положення про академічну мобільність студентів (https://bit.ly/3oMzMkk), власне право неформальну освіту, здобувач може отримати найвищу кількість балів за виконання ІНДЗ, якщо взяв участь у тренінгу, конференції, науковому семінарі, проблемній групі та ін.

Здобувач вчасно здає усі види робіт. Викладач інформує про терміни здачі контрольних робіт та виконання ІНДЗ.

Здобувач має можливість скласти іспит згідно розкладу заліково-екзаменаційної сесії, має право скласти іспит повторно, а також скласти іспит комісії, у яку входять представники кафедри та деканату. Якщо за ці три можливості іспит не складено, здобувач виключається зі складу студентів ВНУ імені Лесі Українки. В університетських положеннях є право на поновлення і проходження повторного проходження навчальної дисципліни.

9.1. Розподіл балів, які отримують студенти

Методи навчання: усне опитування, інтерактивні методи навчання, лабораторні заняття, самостійна робота і екзамен.

Засоби діагностики успішності: лабораторні заняття (30 балів), бонусні бали за активність (10), самостійна робота (30 балів), екзамен (40 балів).

Поточний контроль (мах – 30 балів) Лабораторні заняття	Самостійна робота (мах – 30 балів)	Екзамен (мах – 40 балів)	Загальна кількість балів
30 годин лабораторних занять (мах 30 балів) + 10 балів за активність	67 годин (мах 30 балів)	(мах 40 балів)	100

10. Шкала оцінювання (національна та ECTS)

Сума балів за всі види навчальної діяльності	**Оцінка ECTS**	**Оцінка за національною шкалою**	
		для екзамену, курсової роботи (проекту), практики	**для заліку**
90-100	**A**	**Відмінно**	**Зараховано**
82-89	**B**	**Добре**	
75-81	**C**		
67-74	**D**	**Задовільно**	
60-66	**E**		
1-59	**Fx**	**Незадовільно**	**Незараховано**

РЕКОМЕНДОВАНІ ДЖЕРЕЛА

1. Закон України. Про основні засади забезпечення кібербезпеки України. Введено в дію постановою Верховної Ради України від 05.10. 2017 р. № 45, ст.403.
2. ISO/IEC 11770-3 Information Technology – Security techniques – Key management – Part 3: Mechanisms using asymmetric techniques. January 2007.
3. ISO/IEC 14888-3 Information technology – Security techniques – Digital signatures with appendix – Part 3: Discrete logarithm based Mechanisms. June 2006.
4. НД ТЗІ 2.1-001-2001 Створення комплексів технічного захисту інформації. Атестація комплексів. Основні положення. Затверджено наказом ДСТСЗІ СБ України від 09.02.2001 № 2.
5. Serhii Yevseiev, Volodymir Ponomarenko, Oleksandr Laptiev, Oleksandr Milov and others/ Synergy of building cybersecurity systems. Kharkiv. Publisher PC TECHNOLOGY CENTER. 2021 – 188 c.
6. Лаптєв О.А., Савченко В.А., Шуклін Г.В. Виявлення та блокування засобів негласного отримання інформації на об'єктах інформаційної діяльності. К. ДУТ. 2020 – 126 с. https://dut.edu.ua/ua/lib/2/category/96/view/2031
7. О.А. Лаптєв. Методологічні основи автоматизованого пошуку цифрових засобів негласного отримання інформації. – К. Міленіум. 2020 – 326 с. УДК 004.056.53. ISBN 987-966-8063-79-3. https://www.dut.edu.ua/uploads/l_2162_16683938.pdf
8. Лаптєв О.А., Кузавков В.В., Хорошко В.О. «Системи пошуку засобів негласного здобуття акустичної інформації» – К. Міленіум. 2023 – 282 с. https://www.researchgate.net/publication/368925556_SISTEMI_POSUKU_ZASOBIV_NEGLASNOGO_ZDOBUTTA_AKUSTICNOI_INFORMACII

Додаткова література:

1. Богуш В.М., Кудін А.М. Моніторинг і аудит систем інформаційної безпеки. К.: ДУІКТ, 2006, – 340 с.
2. Указ Президента України №446/2021 Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про невідкладні заходи з кібероборони держави"
3. НД ТЗІ 1.1-003-99 Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу. Затверджений наказом ДСТСЗІ СБУ от 28.04.99 № 22. Діє від 01.07.99.
4. НД ТЗІ 2.1-001-2001 Створення комплексів технічного захисту інформації. Атестація комплексів. Основні положення. Затверджено наказом ДСТСЗІ СБ України від 09.02.2001 № 2.
5. НД ТЗІ 3.7-003-05 Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі Затверджено наказом ДСТСЗІ СБ України від 08.11.05.

Додаткові джерела:

1. A.O. Korchenko, V.O. Breslavskyi, S.P Yevseiev, N.K. Zhumangalieva, A.O. Zvarych, S.V. Kazmirchuk, O.A. Kurchenko, O.A. Laptiev, O. V. Severinov, S. S. Tkachuk. Development of a method for construction of linguistic standards for multicriterial evaluation of HONEYPOT efficiency. Eastern-European journal of enterprise technologies. Vol.1№2 (109), 2021 pp. 14–23. ISSN (print)1729 - 3774. ISSN (on-line) 1729-4061. DOI: 10.15587/1729-4061.2021.225346.
2. Serhii Yevseiev, Oleksandr Laptiev, Sergii Lazarenko, Anna Korchenko, Iryna Manzhul. Modeling the protection of personal data from trust and the amount of information on social networks. Number 1 (2021), «EUREKA: Physics and Engineering» pp.24–31. DOI:10.21303/2461-4262.2021.001615.