МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Волинський національний університет імені Лесі Українки
Факультет інформаційних технологій і математики
Кафедра комп'ютерних наук та кібербезпеки

СИЛАБУС

нормативного освітнього компонента

ПРОЕКТУВАННЯ СИСТЕМ ТЕХНІЧНОГО ЗАХИСТУ

Підготовки першого (бакалаврського) рівня вищої освіти
Спеціальності 125 Кібербезпека та захист інформації
Освітньо-професійної програми Кібербезпека та захист інформації

Луцьк 2023

Силабус нормативного освітнього компонента «Проектування систем технічного захисту» підготовки бакалавра, галузі знань 12 Інформаційні технології, спеціальності 125 Кібербезпека та захист інформації, за освітньою програмою Кібербезпека та захист інформації.

Розробник: Новосад Олексій Володимирович, доцент кафедри комп'ютерних наук та кібербезпеки, к. ф.-м. н.

Погоджено

Гарант освітньо-професійної програми:  Глинчук Л.Я.

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

протокол № 2 від 28.09.2023 р.

Завідувач кафедри:  Гришанович Т. О.

І. Опис освітнього компонента

<table>
<tr><th>Найменування показників</th><th>Галузь знань, спеціальність, освітньо-професійна програма, освітній ступінь</th><th>Характеристика навчальної дисципліни</th></tr>
<tr><td rowspan="2">Денна форма навчання</td><td rowspan="7">Галузь знань
12 Інформаційні технології,
спеціальність
125 Кібербезпека та захист інформації,
освітньо-професійна програма
Кібербезпека та захист інформації
освітній рівень бакалавр.</td><td>Нормативна</td></tr>
<tr><td>Рік навчання 4</td></tr>
<tr><td rowspan="2">Кількість годин/кредитів
120/4</td><td>Семестр 8-й</td></tr>
<tr><td>Лекції 38 год.</td></tr>
<tr><td rowspan="3">ІНДЗ: немає</td><td>Лабораторні роботи 48</td></tr>
<tr><td>Самостійна робота 26 год.</td></tr>
<tr><td>Консультації 8 год.</td></tr>
<tr><td colspan="2">Мова викладання</td><td>Українська</td></tr>
<tr><td colspan="2"></td><td>Форма контролю: екзамен</td></tr>
</table>

ІІ. Інформація про викладача

ПІП: Новосад Олексій Володимирович
Науковий ступінь: кандидат фіз.-мат. наук
Вчене звання: доцент
Посада: доцент кафедри комп'ютерних наук та кібербезпеки
Контактна інформація: тел. 0669348463, e-mail: novosad.oleksiy@vnu.edu.ua
Дні занять: http://94.130.69.82/cgi-bin/timetable.cgi

ІІІ. Опис освітнього компонента

1. Анотація освітнього компонента

Освітній компонент «**Проектування систем технічного захисту**» в системі підготовки здобувачів освіти бакалаврського рівня спеціальності 125 «Кібербезпека» належить до освітніх компонент циклу професійної підготовки. Даний освітній компонент дозволяє опанувати методи проєктування комплексних систем захисту інформації в інформаційно-телекомунікаційних ситемах. Розглядаються окремі питання упровадження та супроводу комплексних систем захисту інформації.

2. Мета і завдання освітнього компонента

Метою освітнього компонента «**Проєктування систем технічного захисту**» є набуття здобувачами освіти теоретичних знань та практичних навичок з проєктування, впровадження та супроводу комплексних систем захисту інформації в інформаційно-телекомунікаційних ситемах.

Основним **завданням** освітнього компонента є вивчення здобувачами освіти основних джерел та шляхів витоку інформації; способів несанкціонованого перехоплення інформації; основних технічних засобів, що використовуються для несанкціонованого

перехоплення інформації; методів та засобів захисту інформації; основних технічних засобів, що використовуються для захисту інформації від несанкціонованого перехоплення; порядку проєктування системи захисту інформації.

3. Результати навчання (компетентності)

Загальні компетентності

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.

Фахові компетентності

ФК 2. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки.

ФК 3. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах.

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 12. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки.

Програмні результати навчання

ПРН 3. Використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності.

ПРН 4. Аналізувати, аргументувати, приймати рішення при розв’язанні складних спеціалізованих задач та практичних проблем у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення.

ПРН 6. Критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності.

ПРН 10. Виконувати аналіз та декомпозицію інформаційно-телекомунікаційних систем.

ПРН 12. Розробляти моделі загроз та порушника.

ПРН 13. Аналізувати проекти інформаційно-телекомунікаційних систем базуючись на стандартизованих технологіях та протоколах передачі даних.

ПРН 17. Забезпечувати процеси захисту та функціонування інформаційно-телекомунікаційних автоматизованих) систем на основі практик, навичок та знань, щодо структурних (структурно-логічних) схем, топології мережі, сучасних архітектур та моделей захисту електронних інформаційних ресурсів з відображенням взаємозв’язків та інформаційних потоків, процесів для внутрішніх і віддалених компонент.

ПРН 19. Застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах.

ПРН 22. Вирішувати задачі управління процедурами ідентифікації, аутентифікації, авторизації процесів і користувачів в інформаційно- телекомунікаційних системах згідно встановленої політики інформаційної і\або кібербезпеки.

ПРН 27. Вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах.

ПРН 29. Здійснювати оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційно-телекомунікаційних системах та ефективності використання комплексів засобів захисту в умовах реалізації загроз різних класів.
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.

4. Структура освітнього компонента

Назви змістових модулів і тем	Усього	Лек.	Лаб. роб.	Сам. роб.	Конс.	Форма контр./ Бали
Змістовий модуль 1. Основні принципи захисту від загроз						
Тема 1. Основні принципи та етапи захисту від загроз. Нормативно-правове забезпечення захисту інформації.	6	2	2	1	1	ЛР/2
Тема 2. Етапи створення КСЗІ в ІТС.	5	2	2	1		ЛР/2
Тема 3. Формування вимог до КСЗІ (1-й етап).	6	2	2	2		ЛР/2
Тема 4. Канали витоку інформації.	6	2	2	1	1	ЛР/2
Тема 5. Складання моделі порушника безпеки інформації в ІТС.	8	2	4	2		ЛР/2
Тема 6. Складання моделі загроз для інформації в ІТС	7	2	4	1		ЛР/2
Тема 7. Формування завдання та варіанту побудови КСЗІ.	7	2	2	2	1	ЛР/2
Тема 8. Основні вимоги до комплексів засобів захисту від НСД	5	2	2	1		ЛР/2
Тема 9. Побудова і структура послуг безпеки інформації.	6	2	2	2		ЛР/2
Тема 10. Побудова і структура гарантій реалізації послуг безпеки.	6	2	2	1	1	ЛР/2
Разом за модулем 2	**62**	**20**	**24**	**14**	**4**	**20**
Змістовий модуль 2. Основні етапи створення КСЗІ						
Тема 11. Вимоги щодо захисту інформації від НСД в АС класу 1	6	2	2	1	1	ЛР/2
Тема 12. Особливості захисту секретної інформації в АС класу 1	5	2	2	1		ЛР/2
Тема 13. Розробка політики безпеки інформації в ІТС (2-й етап).	6	2	2	2		ЛР/2
Тема 14. Складання плану захисту інформації в ІТС.	6	2	2	1	1	ЛР/2
Тема 15. Вибір операційної системи,	5	2	2	1		ЛР/2

АВПЗ і КЗЗ						
Тема 16. Опис КЗЗ від НСД, що мають експертні висновки.	6	2	2	2		ЛР/2
Тема 17. Технічне завдання на створення КСЗІ (3-й етап).	6	2	2	1	1	ЛР/2
Тема 18. Проектування КСЗІ в ІТС (4-й етап).	9	2	6	1		ЛР/4
Тема 19. Введення КСЗІ в дію та оцінка захищеності інформації (5-й етап). Супровід КСЗІ в ІТС (6-й етап).	7	2	2	2	1	ЛР/2
Разом за модулем 2	**58**	**18**	**24**	**12**	**4**	**20**
Види підсумкових робіт						**Бал**
Модульна контрольна робота 1						30
Модульна контрольна робота 2						30
Всього годин / Балів	**120**	**38**	**48**	**26**	**8**	**100**

Форма контролю*: ДС–дискусія, ДБ–дебати, Т–тести, ТР–тренінг, РЗ/К–розв'язування задач/кейсів, ІНДЗ/ІРС–індивідуальне завдання/індивідуальна робота студента, ЛР - лабораторна робота РМГ–робота в малих групах, МКР/КР–модульна контрольна робота/контрольна робота.

5. Самостійна робота

Самостійна робота здобувачів освіти включає в себе:

Опрацювання лекційного матеріалу - 10 год. Перевірка здійснюється під час лабораторних робіт та оцінюється при виставленні оцінки за змістовий модуль.

Підготовка до лабораторних робіт - 10 год. Перевірка здійснюється під час лабораторних робіт.

Систематизація вивченого матеріалу перед модульними контрольними роботами - 6 год. Перевірка здійснюється під час контрольних заходів.

6. Політика оцінювання

Відвідування лекцій та відсутність на них здобувачів вищої освіти не оцінюється. Однак, рекомендується здобувачам освіти відвідувати лекційні заняття, оскільки на них докладно викладається теоретичний матеріал та розвиваються практичні навички, необхідні для успішного завершення курсу. Система оцінювання даного освітнього компонента орієнтована на отримання балів за активність здобувача вищої освіти, а також виконання ним завдань, які здатні розвинути практичні уміння та навички.

Політика щодо дедлайнів та перескладання. Робота вважається виконаною вчасно, якщо викладач отримав звіт з її виконання не пізніше кінця доби наступної лабораторної чи практичної роботи. У випадку, якщо здобувач освіти не відвідував окремі аудиторні заняття (з поважних причин), на консультаціях він має право відпрацювати пропущені заняття та добрати ту кількість балів, яку було визначено на пропущені теми.

Контрольні заходи впродовж навчання реалізуються двома модульними контрольними роботами (які оцінюються 30 балами кожна).

Роботи, які містять плагіат оцінюються нульовим балом. Під час виконання практичних робіт, підсумкових робіт та інших видів навчальної діяльності здобувач вищої освіти повинен дотримуватися правил академічної доброчесності. Правила академічної доброчесності описані у статті 42 Закону України Про Освіту (https://zakon.rada.gov.ua/rada/show/v-650729-18#Text) та у Кодексі академічної доброчесності Волинського національного університету імені Лесі Українки

(http://ra.vnu.edu.ua/wp-content/uploads/2020/03/Academ_Dobr_Code.docx).

Здобувач вищої освіти має право оскаржити результати оцінювання його діяльності шляхом написання листа на ім'я декана факультету, у якому аргументовано вказано з яким значенням оцінки його діяльності він не погоджується.

Згідно «Положення про визнання результатів навчання, отриманих у формальній, неформальній та/або інформальній освіті у Волинському національному університеті імені Лесі Українки» від 11 вересня 2020 року здобувачу вищої освіти можуть бути зарахованими результати навчання, які отримані у формальній, неформальній та/або інформальній освіті.

У даному курсі передбачено заохочувальні бали за наукову діяльність здобувача освіти, які становлять у сумі не більше 10 балів. За публікацію тез доповідей на конференції додатково нараховується 3 бали, за публікацію статті у фаховому виданні 7 балів.

7. Підсумковий контроль

У процесі вивчення дисципліни використовуються такі методи оцінювання навчальної роботи здобувача вищої освіти:

- поточне тестування та опитування;
- виконання та захист лабораторних робіт;
- модульні контрольні роботи;
- питання на екзамен.

Діагностика залишкових базових знань з дисципліни проводиться з використанням модульних контрольних робіт, підготовлених викладачем.

Підсумковий бал (за 100-бальної шкалою) з курсу визначається так:

- кількість балів за поточне оцінювання (практичні роботи) – 40 балів;
- модульний контроль – 60 балів (модульна контрольна робота 1 – 30 балів та модульна контрольна робота 2 – 30 балів).

Модульний контроль/іспит проводяться у письмовій формі. Білет містить завдання різної складності із зазначенням кількості балів за кожне завдання. Після перевірки здобувач освіти отримує роботу із зауваженнями викладача та підсумковою оцінкою.

За згодою здобувача освіти підсумкова семестрова оцінка виставляється без складання іспиту за результатами поточного і модульного контролю у випадку, якщо він успішно виконав усі завдання, передбачені силабусом, і набрав при цьому не менше, як 75 балів.

У випадку незадовільної підсумкової семестрової оцінки або за бажанням підвищити рейтинг, здобувач складає іспит у формі тестового контролю. У цьому випадку на іспит виноситься 60 балів, а бали, набрані за результатами модульних контрольних робіт, анулюються. Остаточна кількість балів буде рівна сумі балів, набраних здобувачем освіти за поточне оцінювання, та кількості балів, набраних на іспиті.

Перелік питань на екзамен

1. Головні принципи та етапи захисту від загроз.
2. Нормативно-правове забезпечення захисту інформації.
3. Організаційні засади забезпечення захисту інформації.
4. Етапи створення КСЗІ в ІТС.
5. Формування вимог до КСЗІ (1-й етап).
6. Категоріювання ІТС.

7. Обстеження середовищ функціонування ІТС.
8. Модель порушника безпеки інформації в ІТС.
9. Модель загроз для інформації в ІТС.
10. Перелік загроз з визначенням порушень властивостей інформації та ІТС.
11. Модель загроз з визначенням рівня ризиків та збитків.
12. Загрози цілісності інформації.
13. Загрози доступності інформації.
14. Загрози спостереженості ІТС.
15. Індикатори електромагнітних випромінювань.
16. Радіочастотоміри.
17. Автоматизовані пошукові комплекси.
18. Мобільні пошукові комплекси.
19. Скануючі приймачі.
20. Спеціалізоване програмне забезпечення.
21. Тепловізорні засоби.
22. Стаціонарні комплекси автоматичного виявлення радіомікрофонів.
23. Типові методи та прийоми проектування захищених інформаційних та комунікаційних систем.
24. Формування завдання на створення КСЗІ.
25. Аналіз ризиків реалізації загроз.
26. Основні вимоги до розробки комплексу засобів захисту.
27. Побудова і структура послуг безпеки інформації.
28. Побудова і структура гарантій реалізації послуг безпеки.
29. Типові умови функціонування АС.
30. Визначення функціональний профіль захищеності.
31. Загальна характеристика технічних каналів витоку інформації, що обробляється в АС.
32. Електричні канали витоку інформації.
33. Електромагнітні канали витоку інформації .
34. Радіоканали втрат інформації.
35. Технічні канали витоку інформації на основі закладних пристроїв.
36. Системи блокування відеоспостереження.
37. Канали витоку інформації при експлуатації ЕОМ.
38. Фізична і апаратна безпека IoT.
39. Вібраційні канали витоку акустичної інформації.
40. Електроакустичні канали витоку акустичної інформації.
41. Оптико-електронний канал витоку акустичної інформації, його характеристика, методи блокування.
42. Індукційний метод перехоплення інформації при її передачі по каналах зв’язку.
43. Класифікація, принцип роботи акустичних закладок.
44. Класифікація, принцип роботи віброакустичних закладок.
45. Класифікація, принцип роботи спрямованих мікрофонів.
46. Класифікація, принцип роботи панорамних скануючих приймачів.
47. Класифікація, принцип роботи аналізаторів спектру та пеленгаторів.
48. Програмно-апаратні комплекси радіо-, радіотехнічної розвідки.
49. Засоби візуальної розвідки.

50. Системи спостереження за транспортними засобами. Радіомаяки. Радіонавігаційний приймач.
51. Класифікація методів та засобів захисту інформації від витоку технічними каналами.
52. Засоби виявлення, локалізації і нейтралізації закладних пристроїв
53. Створення комплексу технічного захисту інформації.
54. Розробка політики безпеки інформації в ІТС (2-й етап).
55. Вибір ОС, АВПЗ.
56. Вибір КЗЗ від НСД.
57. Системи захисту Web-ресурсів.
58. Вибір комплексу ТЗІ.
59. Опис функцій і можливостей КЗЗ від НСД.
60. Технічне завдання на створення КСЗІ (3-й етап).
61. Проектування КСЗІ в ІТС (4-й етап).
62. Введення КСЗІ в дію та оцінка захищеності інформації (5-й етап).
63. Супровід КСЗІ в ІТС (6-й етап).

Шкала оцінювання знань здобувачів освіти

Оцінка в балах	**Лінгвістична оцінка**	**Оцінка за шкалою ECTS**	
		оцінка	**пояснення**
90–100	Відмінно	A	відмінне виконання
82–89	Дуже добре	B	вище середнього рівня
75-81	Добре	C	загалом хороша робота
67-74	Задовільно	D	непогано
60-66	Достатньо	E	виконання відповідає мінімальним критеріям
1–59	Незадовільно	Fx	необхідне перескладання

8. Рекомендована література та інтернет-ресурси

1. Іванченко С.О., Гавриленко О.В., Липський О.А., Шевцов А.С. Технічні канали витоку інформації. Порядок створення комплексів технічного захисту інформації. Навчальний посібник. К.: ІСЗЗІ НТУУ «КПІ», 2016. 104 с. Режим доступу: https://ela.kpi.ua/handle/123456789/15155 (дата звернення: 20.08.2023).

2. Поради (рекомендації) щодо створення КСЗІ в ІКС, які використовуються для надання послуг доступу до мережі Інтернет. Режим доступу: https://cip.gov.ua/ua/news/poradi-rekomendaciyi-shodo-stvorennya-kszi-v-its-yaki-vikoristovuyutsya-dlya-nadannya-poslug-dostupu-do-merezhi-internet (дата звернення: 20.08.2023).

3. Ластівка Г. І., Шпатар П. М. Технічний захист інформації в інформаційних та телекомунікаційних системах: Навчальний посібник. Чернівці: Чернівецький національний університет, 2018. 252 с. Режим доступу: http://radiotech.cv.ua/documents/book/KONSPEKT_KANAL.pdf (дата звернення: 20.08.2023).

4. Бобало Ю.Я., Горбатий І.В., Кіселичник М.Д., Бондарєв А.П. та ін. Інформаційна безпека: навчальний посібник. Львів: Видавництво Львівської політехніки, 2019. 580 с. Режим доступу:

https://drive.google.com/file/d/1jACvCh2O4duJOYA3uLUID8cdVf2EFSWU/view?usp=sharing (дата звернення: 20.08.2023).

5. Джулій В. М., Кльоц Ю. П., Муляр І. В., Чешун В. М. Методи і алгоритми захисту інформаційних ресурсів комп'ютерних систем: навчальний посібник. Хмельницький: ХмНУ, 2020. 196 с. Режим доступу: https://drive.google.com/file/d/1-mFMuTkL5VnBgh1bXNfD6nODchxWI4U/view?usp=sharing (дата звернення: 20.08.2023).

6. Saqib Ali, Taiseera Al Balushi, Zia Nadir, Omar Khadeer Hussain. Cyber Security for Cyber Physical Systems. Cham, Switzerland : Springer, 2018. 174 p. Режим доступу: https://www.pdfdrive.com/cyber-security-for-cyber-physical-systems-d187690371.html (дата звернення: 20.08.2023).

7. Michael Schwartz, Maciej Machulak. Securing the Perimeter: Deploying Identity and Access Management with Free Open Source Software Level. Apress, 2018. 377 p. Режим доступу: https://www.pdfdrive.com/securing-the-perimeter-deploying-identity-and-access-management-with-free-open-source-software-e176342517.html (дата звернення: 20.08.2023).

8. Гребенніков В.В. Комплексні системи захисту інформації: проєктування, впровадження, супровід. Ужгород: Ужгородський національний університет, 2013. – 161 с.

9. Закон України "Про інформацію". 2. Закон України "Про захист інформації в інформаційно-телекомунікаційних системах".

10. Закон України "Про основи національної безпеки".

11. Постанова Кабінету Міністрів України від 27.11.1998 № 1893 «Про затвердження Інструкції про порядок обліку, зберігання і використання документів, справ, видань та інших матеріальних носіїв інформації, які містять службову інформацію».

12. ДСТУ 33960-96 Захист інформації. Технічний захист інформації. Основні положення.

13. ДСТУ 33961-96 Захист інформації. Технічний захист інформації. Порядок проведення робіт.

14. ДСТУ 33962-97 Захист інформації. Технічний захист інформації. Терміни та визначення;

15. НД ТЗІ 1.1-005-07 Захист інформації на об’єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Основні положення.

16. НД ТЗІ 1.4-001-2000. Типове положення про службу захисту інформації в автоматизованій системі.

17. НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу.

18. НД ТЗІ 2.5-005-99. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу.

19. НД ТЗІ 3.7-003-05. Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі.

20. НД ТЗІ 3.7-001-99. Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в АС.

21.15. НД ТЗІ 1.6-004-2013 Захист інформації на об’єктах інформаційної діяльності. Положення про категоріювання об’єктів, де циркулює інформація з обмеженим доступом, що становить державну таємницю.

22. НД ТЗІ 1.6-005-2013 Захист інформації на об’єктах інформаційної діяльності. Положення про категоріювання об’єктів, де циркулює інформація з обмеженим доступом, що не становить державної таємниці.