ДЕРЖАВНИЙ ВИЩИЙ НАВЧАЛЬНИЙ ЗАКЛАД
«УЖГОРОДСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ»
ФІЗИЧНИЙ ФАКУЛЬТЕТ
Кафедра твердотільної електроніки та інформаційної безпеки

‹‹ЗАТВЕРДЖУЮ››
Декан фізичного факультету
_____/ Лазур В. Ю.
‹‹_30_›› _червня_ 2023 року

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

«КОМПЛЕКСНІ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ: ПРОЕКТУВАННЯ, ВПРОВАДЖЕННЯ, СУПРОВІД»

Рівень вищої освіти:	**перший (бакалаврський) рівень**
Галузь знань	**12 Інформаційні технології**
Спеціальність	**125 Кібербезпека**
Предметна спеціальність (Спеціалізація) (за наявності)	
Освітня програма	**Безпека інформаційних і комунікаційних систем**
Статус дисципліни	**обов'язкова**
Мова навчання	**українська**

Ужгород 2023

Робоча програма навчальної дисципліни «**Комплексні системи захисту інформації: проектування, впровадження, супровід**» для здобувачів вищої освіти галузі знань **12 Інформаційні технології** спеціальності **125 Кібербезпека** освітньої програми **Безпека інформаційних і комунікаційних систем.**

Розробники: Трикур І. І., к. ф.-м. н, доцент кафедри ТЕІБ.
Чобаль О.І., к. ф.-м. н, доцент кафедри ТЕІБ.

Робочу програму розглянуто та затверджено на засіданні кафедри ***твердотільної електроніки та інформаційної безпеки***

протокол № 9 від « 15 » червня 2023 р.

Завідувач кафедри _____ Різак В.М.

Схвалено науково-методичною комісією фізичного факультету

протокол № 10 від « 28 » червня 2023 р.

Голова науково-методичної комісії _____ Карбованець М. І.

© Трикур І. І., 2023 р.
© Чобаль О. І., 2023 р.
© ДВНЗ «Ужгородський національний університет», 2023 р.

1. ОПИС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

<table>
<tr><th rowspan="2">Найменування показників</th><th>Розподіл годин за навчальним планом</th></tr>
<tr><td>Денна форма навчання</td></tr>
<tr><td>Кількість кредитів ЄКТС – 8</td><td>Рік підготовки:</td></tr>
<tr><td>Загальна кількість годин – 240</td><td>4</td></tr>
<tr><td>Кількість модулів – 4</td><td>Семестр:</td></tr>
<tr><td rowspan="5">Тижневих годин для денної форми навчання:
аудиторних
7-й семестр - 3,3;
8-й семестр - 4,4;
самостійної роботи студента
7-й семестр - 3,3;
8-й семестр - 7,6;</td><td>7,8</td></tr>
<tr><td>Лекції:</td></tr>
<tr><td>54</td></tr>
<tr><td>Практичні (семінарські):</td></tr>
<tr><td>-</td></tr>
<tr><td rowspan="2">Вид підсумкового контролю:
залік, екзамен</td><td>Лабораторні:</td></tr>
<tr><td>50</td></tr>
<tr><td rowspan="2">Форма підсумкового контролю:
усний</td><td>Самостійна робота:</td></tr>
<tr><td>136</td></tr>
</table>

2. МЕТА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Метою вивчення навчальної дисципліни **«Комплексні системи захисту інформації: проектування, впровадження, супровід»** є формування у здобувачів теоретичних знань та практичних навичок створення систем комплексного захисту інформації на об'єктах інформаційної діяльності різного типу, розробка та супровід нормативно-правових документів для таких систем, узгодження параметрів КСЗІ з національними та міжнародними стандартами. В рамках курсу здобувачі отримують поглиблені знання про теоретичні аспекти та засвоюють практичні навички щодо основних етапів створення комплексної системи захисту інформації, її атестації та супроводу її роботи. Під час виконання курсового проекту студенти мають можливість використати отримані знання для організації служби захисту та створення комплексної системи захисту на вибраному модельному об'єкті інформаційної діяльності, підготувати всі необхідні документи, розробити політику інформаційної безпеки, розробити модель порушника та модель загроз інформації.

Відповідно до освітньої програми, вивчення дисципліни сприяє формуванню у здобувачів вищої освіти таких компетентностей: здатність застосовувати знання в практичних ситуаціях (ЗК 1); знання та розуміння предметної області та розуміння професійної діяльності (ЗК 2); вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням (ЗК 4); здатність виявляти суспільно значимі ІТ потреби для їх подальшого задоволення через створення та впровадження сучасних методів і моделей інформаційної безпеки та/або кібербезпеки (ЗК 8); здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі (ФК1); здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки (ФК2); здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної безпеки (ФК 4); здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження (ФК6); здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.) (ФК7); здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку (ФК 8); здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою (ФК 9); здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності (ФК 10); здатність застосовувати теоретичні знання та практичні навички із побудови, керування, модернізації, моніторингу та аналізу продуктивності сучасних інформаційних і комунікаційних систем та мереж (ФК 14).

3. ПЕРЕДУМОВИ ДЛЯ ВИВЧЕННЯ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Враховуючи послідовність накопичення знань та інформації, дисципліна «**Комплексні системи захисту інформації: проектування, впровадження, супровід**» вивчається після опанування студентами наступних дисциплін: «Технології програмування», «Інформаційно-комунікаційні системи», «Інформаційні банківські технології», «Програмні методи та засоби ЗІ», «Організація баз даних і знань».

4. ОЧІКУВАНІ РЕЗУЛЬТАТИ НАВЧАННЯ

Відповідно до освітньої програми **«Комплексні системи захисту інформації: проектування, впровадження, супровід»,** вивчення навчальної дисципліни повинно забезпечити досягнення здобувачами вищої освіти таких програмних результатів навчання (ПРН)**:**

Програмні результати навчання	Шифр ПРН
Готувати пропозиції до нормативних актів щодо забезпечення інформаційної та/або кібербезпеки.	ПРН 8
Виконувати аналіз та декомпозицію інформаційно-телекомунікаційних систем.	ПРН 10
Розробляти моделі загроз та порушника.	ПРН 12
Використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій.	ПРН 15
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 17
Застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах.	ПРН 19
Вирішення задач забезпечення та супроводу (в. т. числі: огляд, тестування, підзвітність) системи управління доступом згідно встановленої політики безпеки в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах.	ПРН 21
Реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах.	ПРН 23
Впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем на основі еталонної моделі взаємодії відкритих систем.	ПРН 26
Аналізувати та проводити оцінку ефективності та рівня захищеності ресурсів різних класів в інформаційних та інформаційно- телекомунікаційних (автоматизованих) системах в ході проведення випробувань згідно встановленої політики інформаційної та\або кібербезпеки.	ПРН 28
Застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем.	ПРН 31
Приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації.	ПРН 34
Виявляти небезпечні сигнали технічних засобів.	ПРН 36
Проводити атестацію (спираючись на облік та обстеження) режимних територій (зон), приміщень тощо в умовах додержання режиму секретності із фіксуванням результатів у відповідних документах.	ПРН 39
Забезпечувати неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур.	ПРН 41
Вирішувати задачі забезпечення безперервності бізнес-процесів організації на основі теорії ризиків та встановленої системи управління інформаційною безпекою, згідно з вітчизняними та міжнародними вимогами та стандартами.	ПРН 44
Використовувати інструментарій для моніторингу процесів в інформаційно-телекомунікаційних системах.	ПРН 52
Здатність демонструвати знання та розуміння основ побудови комп'ютерних систем захисту інформації та описувати в загальних поняттях і термінах архітектуру, характеристики та принципи їх дії.	ПРН 55

Очікувані результати навчання, які повинні бути досягнуті здобувачами освіти після опанування навчальної дисципліни «**Комплексні системи захисту інформації: проектування, впровадження, супровід**»:

Очікувані результати навчання з дисципліни	**Шифр ПРН**
Вміти виконувати аналіз та оцінку інформаційних потоків в інформаційно-телекомунікаційних систем, який дозволяє максимально ефективно використовувати наявні ресурси (та подавати керівництву пропозиції щодо їх розширення чи оптимізації) для забезпечення захисту інформації на всіх етапах її обробки.	ПРН 10, ПРН 34
Вміти аналізувати інформаційне середовище та розробляти моделі загроз інформації, моделі порушника інформації та політику інформаційної безпеки.	ПРН 12, ПРН 21, ПРН 28, ПРН 34
Використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій та відповідні методологічні прийоми для забезпечення інформаційної безпеки.	ПРН 15, ПРН 17, ПРН 19, ПРН 21, ПРН 31
Розробляти, готувати та подавати керівництву відповідні нормативно-правові документи що стосуються створення та функціонування комплексних систем захисту інформації.	ПРН 8, ПРН 39, ПРН 41
Реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів, вести журнали відповідних спроб.	ПРН 23, ПРН 26, ПРН 36, ПРН 41
Вміти реалізовувати задачу неперервності процесу захисту інформації та ефективного управління системою інформаційною безпекою, згідно з вітчизняними та міжнародними вимогами та стандартами.	ПРН 44, ПРН 52
Вміти описувати в загальних поняттях і термінах архітектуру, характеристики та принципи систем захисту інформації для аргументації керівництву необхідності вирішення наявних проблем.	ПРН 55

5. ЗАСОБИ ДІАГНОСТИКИ ТА КРИТЕРІЇ ОЦІНЮВАННЯ РЕЗУЛЬТАТІВ НАВЧАННЯ

Засоби оцінювання та методи демонстрування результатів навчання

Засобами оцінювання та методами демонстрування вивчення дисципліни є:

- стандартизовані тести для поточного контролю засвоєння матеріалу;
- аналітичні звіти по виконаних лабораторних роботах;
- модульні контрольні роботи;
- презентації результатів виконаних завдань та досліджень;
- підсумкові залік у першому та екзамен у другому семестрах;
- представлення результатів виконання та захист курсового проекту;

Форми контролю та критерії оцінювання результатів навчання

Форми поточного контролю: усне опитування, тестування, відповіді на питання для самоконтролю;

Форма модульного контролю: модульні контрольні роботи;

Форма підсумкового семестрового контролю: залік, екзамен

Розподіл балів, які отримують здобувачі вищої освіти (модуль 1)

Поточне оцінювання та самостійна робота								Модульна контрольна робота	Сума
Т1	Т2	Т3	Т4	Т5	Т6	Т7	Т8	50	**100**
10	10	4	2	2	2	10	10		

Т1, Т2 ... – теми

Розподіл балів, які отримують здобувачі вищої освіти (модуль 2)

Поточне оцінювання та самостійна робота							Модульна контрольна робота	Сума
Т1	Т2	Т3	Т4	Т5	Т6	Т7	50	**100**
15	25	2	2	2	2	2		

Т1, Т2 ... – теми

Розподіл балів, які отримують здобувачі вищої освіти (модуль 3)

Поточне оцінювання та самостійна робота					Модульна контрольна робота	Сума
Т1	Т2	Т3	Т4	Т5	50	**100**
2	16	15	2	15		

Т1, Т2 ... – теми

Розподіл балів, які отримують здобувачі вищої освіти (модуль 4)

Поточне оцінювання та самостійна робота				Модульна контрольна робота	Сума
Т1	Т2	Т3	Т4	50	**100**
16	16	2	16		

Т1, Т2 ... – теми

Оцінювання окремих видів навчальної роботи з дисципліни

Вид діяльності здобувача вищої освіти	**Модуль 1**		**Модуль 2**		**Модуль 3**		**Модуль 4**		**Курс. проект**
	К-сть	Макс. к-сть балів (сумарна)	К-сть	Макс. к-сть балів (сумарна)	К-сть	Макс. к-сть балів (сумарна)	К-сть	Макс. к-сть балів (сумарна)	Макс. к-сть балів (сумарна)
Лабораторні заняття (допуск, виконання та захист)	4	34	3	36	3	40	3	42	
Письмове тестування при тематичному оцінюванні	8	16	7	14	5	10	4	8	
Модульна контрольна робота	1	50	1	50	1	50	1	50	
Курсовий проект									100
Разом	**13**	**100**	**11**	**100**	**9**	**100**	8	**100**	**100**

Критерії оцінювання модульної контрольної роботи

Модульний контроль проводиться у вигляді тестування за допомогою ресурсів сайту електронного навчання ДВНЗ "УжНУ" (https://e-learn.uzhnu.edu.ua). Всі питання стосуються матеріалу, який розглядався під час проходження відповідного модулю на лекціях, лабораторних роботах та темах для самостійного вивчення. Тестування складається з 20-ти запитань, які випадковим чином вибираюсь з бази даних питань для поточного контролю по темам що відносяться до даного модуля (в загальному близько 100 запитань завантажених у базу контрольних запитань відповідного модуля відповідного курсу). Питання можуть бути двох типів: для позитивного результати треба обрати одну правильну відповідь або відмітити кілька правильних варіантів із запропонованого переліку. До якого типу відноситься запитання вказується одразу після тексту запитання. Максимальна кількість балів за одне запитання – 5. Якщо запитання передбачає одну правильну відповідь – студенту зараховується 5 балів якщо він обрав правильний варіант, і 0 балів – якщо не правильний. У випадку якщо є кілька правильних відповідей, студент отримує 5 балів у випадку коли відмічені всі правильні варіанти, 0 балів - коли не відмічено жодного правильного варіанту або кількість неправильних відповідей переважає кількість правильних. Якщо відмічено не всі правильні відповіді студенту зараховується бал відповідний відсотку правильно відмічених відповідей. Загальний максимальний бал за модульну контрольну роботу складає 100. Мінімальна кількість набраних балів під час тестування для зарахування здачі контрольної роботи - 60. Якщо здобувач не набирає мінімально кількості балів, йому надається можливість перескласти модульну контрольну роботу у визначений кафедрою термін.

Критерії оцінювання курсової роботи (проекту)

Виконання курсового проекту в рамках дисципліни «**Комплексні системи захисту інформації: проектування, впровадження, супровід**» передбачає розробку пакету документації достатнього для створення КСЗІ на об’єкті інформаційної діяльності (об’єктом зазвичай є організація про яку студент має інформацію – школа де вчився, місце роботи студента чи когось з родини). Виконання курсового проекту оцінюється за 100 бальною шкалою і включає наступні пункти:

№	Назва	Макс. бал.
1	**Змістове наповнення проекту** (наявність у пакеті всіх необхідних згідно стандартів документів, якість розроблених моделей порушника, загроз інформації, оцінки ризиків політики безпеки інформації тощо).	50
2	**Оформлення проекту** (відповідність форми документації регламентованим зразкам, відповідність загального оформлення роботи вимогам до курсових робіт, відсутність помилок та описок);	20
3	**Представлення та захист роботи** (рівень володіння студентом термінологією та матеріалом виконаного дослідження, здатність стисло та коректно презентувати свою роботу, зробити правильні акценти та провести якісний порівняльний аналіз, відмітити головне у висновках).	30
	Разом:	100

Критерії оцінювання підсумкового семестрового контролю

Підсумковий семестровий контроль по даній дисципліні передбачає проведення недиференційованого заліку в кінці сьомого семестру та екзамену в кінці восьмого семестру навчання. Допуском до складання заліку/екзамену вважається виконання та захист всіх лабораторних робіт передбачених програмою у відповідному семестрі та середня модульна оцінка не менше 50 балів (за 100-бальною шкалою).

Оцінювання навчальних досягнень студентів здійснюється за шкалою, наведеною в таблиці.

Шкала оцінювання: національна та ECTS

Сума балів за всі види навчальної діяльності	Оцінка ECTS	Оцінка за національною шкалою	
		для екзамену, курсового проекту (роботи), практики	для заліку
90 – 100	**A**	відмінно	зараховано
82-89	**B**	добре	
74-81	**C**		
64-73	**D**	задовільно	
60-63	**E**		
35-59	**FX**	незадовільно з можливістю повторного складання	не зараховано з можливістю повторного складання
0-34	**F**	незадовільно з обов'язковим повторним вивченням дисципліни	не зараховано з обов'язковим повторним вивченням дисципліни

Якщо підсумкова модульна оцінка становить не менше 60 балів, то, за згодою здобувача, вона може бути зарахована як підсумкова семестрова оцінка з навчальної дисципліни. З метою підвищення рейтингової оцінки здобувач вищої освіти, за бажанням, може складати залік у 7-мому чи екзамен у 8-мому семестрі з дисципліни під час сесії, результат якого визнається остаточним.

Для підвищення оцінки здобувачу пропонується в усній формі відповісти на два теоретичні запитання та виконати одне практичне завдання. Перелік теоретичних запитань та типових практичних завдань надається студентам для підготовки окремо. У випадку правильного виконання практичного завдання, володіння теоретичним матеріалом та правильних відповідей на додаткові запитання здобувач може підвищити підсумкову модульну оцінку. Якщо здобувач освіти не з'явився на залік у визначений час, то у відомості обліку успішності записується його підсумкову модульну оцінку при умові, що вона не менша 60 балів, або «не з'явився», якщо ця оцінка становить менше 60 балів.

Здобувачі освіти, підсумкова модульна оцінка яких становить від 35 до 59 балів або, які за результатами модульних контролів не допущені до їх складання, не з'явилися на екзамен чи залік без поважних причин, вважаються такими, що одержали незадовільну оцінку.

Повторне складання заліків з метою виправлення незадовільної оцінки допускається не більше двох разів з у кожному семестрі: один раз викладачеві, другий - комісії у складі не менше двох осіб, яку формує завідувач кафедри.

6. ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

6.1. Зміст навчальної дисципліни

Модуль 1

Тема 1. Загальні положення про комплексні системи захисту інформації.
Тема 2. Загальні уявлення про заходи по захисту інформації.
Тема 3. Порядок здійснення захисту інформації на об'єктах інформаційної діяльності.
Тема 4. Атестація систем захисту інформації.
Тема 5. Захист інформації від витоку технічними каналами.
Тема 6. Захист інформації під час використання засобів копіювально-розмножувальної техніки.
Тема 7. Головні принципи та етапи захисту від загроз. Нормативно-правове забезпечення захисту інформації.
Тема 8. Нормативні документи ТЗІ, які визначають порядок створення КСЗІ в ІТС.

Модуль 2

Тема 1. Етапи створення КСЗІ. Формування вимог до КСЗІ.

Тема 2. Положення про службу захисту інформації в ІТС.
Тема 3. Модель порушника безпеки інформації в ІТС.
Тема 4. Модель загроз для інформації в ІТС.
Тема 5. Формування завдань та варіанту побудови КСЗІ.
Тема 6. Основні вимоги до розробки комплексу засобів захисту.
Тема 7. Побудова і структура послуг безпеки інформації: послуги конфіденційності та цілісності інформації.

Модуль 3

Тема 1. Побудова і структура послуг безпеки інформації: послуги доступності та спостережності інформації.
Тема 2. Побудова і структура гарантій реалізації послуг безпеки.
Тема 3. Вимоги до захисту інформації від НСД в АС класу «1».
Тема 4. Додаткові вимоги до захисту секретної інформації в АС класу «1».
Тема 5. Вимоги щодо захисту інформації від НСД в АС класу «2».

Модуль 4

Тема 1. 2-й етап. Розробка політики безпеки інформації в ІТС.
Тема 2. План захисту інформації в ІТС.
Тема 3. Вибір ОС, АВПЗ і КЗЗ.
Тема 4. Опис функцій і можливостей КЗЗ від НСД.

6.2. Структура навчальної дисципліни

Назви змістових модулів і тем	Кількість годин: 240					
	Форма навчання: денна					
	Усього	у тому числі				
		лекції	практичні (семінарські)	лабораторні	індивідуальна робота	Самостійна робота
7-й семестр						
Модуль 1						
Тема 1. Загальні положення про комплексні системи захисту інформації.	4	2		2		
Тема 2. Загальні уявлення про заходи по захисту інформації.	12	2		4		6
Тема 3. Порядок здійснення захисту інформації на об'єктах інформаційної діяльності.	8	4				4
Тема 4. Атестація систем захисту інформації.	6	2				4
Тема 5. Захист інформації від витоку технічними каналами.	6	2				4
Тема 6. Захист інформації під час використання засобів копіювально-розмножувальної техніки	6	2				4
Тема 7. Головні принципи та етапи захисту від загроз. Нормативно-правове забезпечення захисту інформації.	10	2		4		4
Тема 8. Нормативні документи ТЗІ, які	10	2		4		4

визначають порядок створення КСЗІ в ІТС.						
Модульна контрольна робота						
Разом за модуль	62	18		14		30
Модуль 2						
Тема 1. Етапи створення КСЗІ. Формування вимог до КСЗІ.	10	2		4		4
Тема 2. Положення про службу захисту інформації в ІТС.	14	2		8		4
Тема 3. Модель порушника безпеки інформації в ІТС.	6	2				4
Тема 4. Модель загроз для інформації в ІТС.	6	2				4
Тема 5. Формування завдань та варіанту побудови КСЗІ.	10	4				6
Тема 6. Основні вимоги до розробки комплексу засобів захисту.	6	2				4
Тема 7. Побудова і структура послуг безпеки інформації: послуги конфіденційності та цілісності інформації.	6	2				4
Модульна контрольна робота						
Разом за модуль	58	16		12		30
8-й семестр						
Модуль 3						
Тема 1. Побудова і структура послуг безпеки інформації: послуги доступності та спостережності інформації.	7	2				5
Тема 2. Побудова і структура гарантій реалізації послуг безпеки.	11	2		4		5
Тема 3. Вимоги до захисту інформації від НСД в АС класу «1».	11	2		4		5
Тема 4. Додаткові вимоги до захисту секретної інформації в АС класу «1».	7	2				5
Тема 5. Вимоги щодо захисту інформації від НСД в АС класу «2».	14	4		4		6
Виконання курсового проекту	15				15	
Модульна контрольна робота						
Разом за модуль	65	12		12	15	26
Модуль 4						
Тема 1. 2-й етап. Розробка політики безпеки інформації в ІТС.	11	2		4		5
Тема 2. План захисту інформації в ІТС.	11	2		4		5
Тема 3. Вибір ОС, АВПЗ і КЗЗ.	7	2				5
Тема 4. Опис функцій і можливостей КЗЗ від НСД.	11	2		4		5
Виконання курсового проекту	15				15	
Модульна контрольна робота						
Модульна контрольна робота						
Разом за модуль	55	8		12	15	20
Разом	240	54		50	30	106

6.3. Теми лабораторних занять

№ з/п	Назва теми	Кількість годин
1	Ознайомлення з термінологією ТЗІ, яка використовується для документального супроводу КСЗІ.	2
2	Підготовка наказу про створення СЗІ на ОІД та «Загальних положень» для типового «Положення про службу захисту інформації».	4
3	Підготовка розділів «Завдання служби захисту інформації» та «Функції служби захисту інформації».	4
4	Підготовка розділу «Повноваження та відповідальність служби захисту інформації» та розділів що регламентують роботу, фінансування та реструктуризацію СЗІ.	4
5	"Плану захисту інформації в АС": підготовка розділів №1 та №2 для вибраного ОІД.	4
6	"Плану захисту інформації в АС": підготовка розділу №3 для вибраного ОІД.	4
7	"Плану захисту інформації в АС": розробка моделі загроз інформації для вибраного ОІД.	4
8	"Плану захисту інформації в АС": розробка моделі порушника для вибраного ОІД.	4
9	"Плану захисту інформації в АС": розробка політики безпеки інформації в АС.	4
10	Підготовка акту категоріювання для ОІД.	4
11	Підготовка акту обстеження ОІД.	4
12	Здійснення класифікації АС та вибір функціональних профілів захищеності.	4
13	Опис функціональних профілів захищеності (типи профілів - згідно варіанту завдання).	4
	Разом	**50**

6.4. Самостійна робота

№ з/п	Назва теми	Кількість годин
1	Основні стратегії захисту інформації.	6
2	Роль політики інформаційної безпеки ОІД.	4
3	Основні принципи організації КСЗІ	4
4	Концептуальні підходи до проектування систем захисту	4
5	Методи виявлення способів впливу на інформацію	4
6	Організаційно - правові заходи щодо охорони державної таємниці	4
7	Контроль функціонування та керування системою захисту інформації	4
8	Порядок контролю за станом технічного захисту інформації	4
9	Засекречування та розсекречування матеріальних носіїв інформації	4
10	Технічні заходи від витоку інформації технічними каналами	4
11	Класифікатор засобів копіювально-розмножувальної техніки	4
12	Основні нормативно-правові акти України	6
13	Нормативні документи системи технічного захисту інформації	4
14	Прийом обстеження середовища функціонування ІТС	4
15	Категоріювання ІТС	5

16	Положення про СЗІ в ІТС	5
17	Приклади моделі порушника для різних ОІД	5
18	Табличне представлення моделі загроз інформації	5
19	Обробка ризиків	6
20	Реалізація КЗЗ	5
21	Концепція диспетчера доступу	5
22	Порядок розроблення та оформлення паспорта на комплекс ТЗІ	5
23	Вимоги до функціональних послуг безпеки інформації	5
	Разом	**106**

7. ІНСТРУМЕНТИ, ОБЛАДНАННЯ ТА ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ, ВИКОРИСТАННЯ ЯКИХ ПЕРЕДБАЧАЄ НАВЧАЛЬНА ДИСЦИПЛІНА

Навчальна дисципліна «**Комплексні системи захисту інформації: проектування, впровадження, супровід**» частково передбачає показ ілюстративного матеріалу та комп'ютерне тестування, для чого використовується відповідне мультимедійне обладнання. Розміщення матеріалів лекцій та завдань для лабораторних робіт, поточне тестування та модульний контроль реалізовано на базі сайту електронного навчання ДВНЗ "УжНУ" (https://e-learn.uzhnu.edu.ua). У випадку дистанційного навчання онлайн-заняття проводяться з використанням платформи Google Meet.

8. РЕКОМЕНДОВАНІ ДЖЕРЕЛА ІНФОРМАЦІЇ

Основна література

1. Комплексні системи захисту інформації: проектування, впровадження, супровід. Збірник лекцій [Електронний ресурс] / Гребенніков В.В. // 2015 - Режим доступу: https://dspace.uzhnu.edu.ua/jspui/handle/lib/10070?locale=uk
2. Комплексні системи захисту інформації : навчальний посібник / К63 [Яремчук Ю. Є., Павловський П. В., Катаєв В. С., Сінюгін В. В.] – Вінниця : ВНТУ, 2018. – 118 с.
3. Закон України. Про основні засади забезпечення кібербезпеки України. Введено в дію постановою Верховної Ради України від 05.10. 2017 р. № 45, ст.403.
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. Комплексні системи захисту інформації. Методичні вказівки до лабораторних занять для здобувачів першого (бакалаврського) рівня освітньої програми 125 «Кібербезпека» денної та заочної форм навчання. / уклад. В.М. Мельник. – Луцьк: Луцький НТУ, 2020. – 22 с.
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
9. Богуш В.М., Кудін А.М. Моніторинг і аудит систем інформаційної безпеки. К.: ДУІКТ, 2006, – 340 с.

10. ISO/IEC 11770-3 Information Technology – Security techniques – Key management – Part 3: Mechanisms using asymmetric techniques. January 2007.
11. І.Д. Горбенко, Т.О. Гріненко. Захист інформації в інформаційно-телекомунікаційних системах: Навч. посібник, Ч.1, Криптографічний захист інформації. – Харків: ХНУРЕ, 2004. – 368 с.

Допоміжна література

1. Указ Президента України №446/2021 Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про невідкладні заходи з кібероборони держави"
2. 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.
3. 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.
4. Хошаба О.М. Частина 13: Захист інформації в системах електронного урядування / Електронне урядування та електронна демократія: навч. посіб.: у 15 ч. / за заг. ред. А.І. Семенченка, В.М. Дрешпака. – К: ФОП Москаленко О. М., 2017. – 72 с.
5. Комплекс засобів захисту від НСД в АС класу 1 «Рубіж-РСО» версія 2 [Електронний ресурс] / ТОВ «Технічний захист інформації» // 2013 - Режим доступу: http://tzi.com.ua/rubzh-rso-versya-20.html
6. Система захисту інформації «ЛОЗА-1». Програмні засоби адміністрування системи. Інструкції. «ТОВ НДІ "Автопром" Київ, 2018».

Інформаційні ресурси в мережі Інтернет

1. Офіційний веб-сайт Верховної Ради України - Режим доступу: http://portal.rada.gov.ua
2. Офіційний веб-сайт Кабінету Міністрів України - Режим доступу: http://kmu.gov.ua
3. Офіційний веб-сайт Президента України http - Режим доступу: http://president.gov.ua
4. Законодавство України - Режим доступу: http://zakon.rada.gov.ua
5. Державна служба спеціального зв'язку та захисту інформації України - Режим доступу: https://cip.gov.ua/ua