МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

МІЖНАРОДНИЙ ГУМАНІТАРНИЙ УНІВЕРСИТЕТ

Кафедра комп'ютерної інженерії та інноваційних технологій

«ЗАТВЕРДЖУЮ»

Ректор Міжнародного гуманітарного університету д.ю.н., професор

_____ Костянтин ГРОМОВЕНКО

«29» серпня 2025 р.

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

КОМПЛЕКСНІ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ

Галузь знань	12 «Інформаційні технології»
Спеціальність	125 «Кібербезпека та захист інформації»
Назва освітньої програми	Кібербезпека та захист інформації
Рівень вищої освіти	перший (бакалаврський) рівень

Одеса – 2025 рік

Робоча програма затверджена на засіданні кафедри комп'ютерної інженерії та інноваційних технологій протокол № 1 від 28.08 2025 року.

Розробники і викладачі	**Контактний тел.**	**E-mail**
доцент кафедри комп'ютерної інженерії та інноваційних технологій к.т.н., доцент **Онацький Олексій Віталійович**	+380503761048	onatsky@meta.ua

Завідувач кафедри комп'ютерної інженерії
та інноваційних технологій
к.т.н., доцент _____ Лариса ЙОНА

Гарант освітньої програми
к.т.н., доцент _____ Лариса ЙОНА

Узгоджено
Начальник навчального відділу _____ Лілія САЄНКО

ОПИС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

<table>
<tr><th rowspan="2">Найменування показників</th><th rowspan="2">Галузь знань, напрям підготовки, освітньо-кваліфікаційний рівень</th><th colspan="2">Характеристика навчальної дисципліни</th></tr>
<tr><th>денна форма навчання</th><th>заочна форма навчання</th></tr>
<tr><td rowspan="10">Кількість кредитів – 5

Загальна кількість годин – 150</td><td>Галузь – 12 Інформаційні технології</td><td colspan="2">обов’язкова</td></tr>
<tr><td rowspan="9">Спеціальність – 125 Кібербезпека та захист інформації</td><td colspan="2">Рік підготовки:</td></tr>
<tr><td colspan="2">3-й</td></tr>
<tr><td colspan="2">Семестр</td></tr>
<tr><td>6-й</td><td>6-й</td></tr>
<tr><td colspan="2">Лекції</td></tr>
<tr><td>26 год.</td><td>6 год.</td></tr>
<tr><td colspan="2">Практичні, семінарські</td></tr>
<tr><td>14 год.</td><td>2 год.</td></tr>
<tr><td colspan="2">Лабораторні</td></tr>
<tr><td>20 год.</td><td>4 год.</td></tr>
<tr><td colspan="2">Самостійна робота та індивідуальні завдання</td></tr>
<tr><td>90 год.</td><td>138 год.</td></tr>
<tr><td colspan="2">Вид контролю:</td></tr>
<tr><td>Екзамен</td><td>Екзамен</td></tr>
</table>

ОК Комплексні системи захисту інформації надає змогу здобувачам першого (бакалаврського) ступеня вищої освіти оволодіти теоретичними знання для задач керування по створенню комплексної системи захисту інформації (КСЗІ), аналізувати потреби та вимоги користувачів з метою планування і створення КСЗІ.

Метою Комплексні системи захисту інформації є формування у здобувачів фундаментальних знань теоретичних та практичних надбань: з проблем захисту інформацій та інформаційних ресурсів в інформаційно-комунікаційних системах (ІКС) та інформаційно-телекомунікаційних системах (ІТС) від порушення її конфіденційності, цілісності та доступності; основ організації та порядку проведення робіт зі створення КСЗІ; етапів створення КСЗІ; формування вимог до КСЗІ, вимогам щодо захисту інформації від несанкціонованого доступу (НСД); проектування КСЗІ ІКС; введення КСЗІ в ІКС в дію та її супровід.

Передумови для вивчення дисципліни. Даний курс ґрунтується на знаннях та навичках курсів «Захисту інформації в інфокомунікаційних системах та мережах» (ОК 12), «Криптографії та криптоаналізу» (ОК 23), «Операційних систем» (ОК 20), «Основ Web-безпеки» (ОК 22) та паралельного вивчення «Безпеки програм та даних» (ОК 16).

2. ОЧІКУВАНІ КОМПЕТЕНТНОСТІ, ЯКІ ПЛАНУЄТЬСЯ СФОРМУВАТИ ТА ДОСЯГНЕННЯ ПРОГРАМНИХ РЕЗУЛЬТАТІВ

У процесі реалізації програми дисципліни «Комплексні системи захисту інформації» формуються наступні компетентності із передбачених освітньою програмою:

Інтегральна компетентність

ІК. Здатність розв'язувати складні спеціалізовані задачі та практичні проблеми у галузі кібербезпеки та захисту інформації.

Загальні компетентності

ЗК 1. Здатність застосовувати знання у практичних ситуаціях.

ЗК 2. Знання та розуміння предметної області та розуміння професійної діяльності

Спеціальні (фахові, предметні) компетентності

СК 4. Здатність забезпечувати захист інформації в інформаційних та інформаційно-комунікаційних системах згідно встановленої політики кібербезпеки й захисту інформації.

СК 6. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів тощо).

СК 8. Здатність застосовувати методи та засоби криптографічного захисту інформації на об'єктах інформаційної діяльності.

СК 9. Здатність застосовувати методи та засоби технічного захисту інформації на об'єктах інформаційної діяльності.

СК 11. Здатність здійснювати проєктування, адміністрування та керування інформаційно-комунікаційними системами, забезпечуючи їхню надійність, безпеку та ефективність функціонування.

Навчальна дисципліна «Комплексні системи захисту інформації» забезпечує досягнення програмних результатів навчання (РН), передбачених освітньою програмою:

РН 9. Знати та застосовувати законодавство України та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі кібербезпеки та захисту інформації

РН 12. Застосовувати методи та засоби захисту інформації в інформаційних та інформаційно-комунікаційних системах відповідно до встановленої політики інформаційної безпеки.

РН 13. Впроваджувати, налаштовувати, супроводжувати та підтримувати функціонування програмних і програмно-апаратних комплексів і систем кібербезпеки та захисту інформації як необхідні процедури для функціонування інформаційних й інформаційно-комунікаційних систем та/або інфраструктури організації в цілому.

РН 16. Вирішувати задачі впровадження та супроводу комплексних систем захисту інформації в інформаційних системах.

РН 17. Забезпечувати функціонування системи управління кібербезпекою і захистом інформації організації, включаючи персонал та управління наслідками реалізації загроз інформаційній безпеці в кризових ситуаціях, на основі здійснення процедур кількісної і якісної оцінки ризиків.

РН 20. Визначати загрози створення технічних каналів витоку інформації на об'єктах інформаційної діяльності; впроваджувати засоби і заходи технічного захисту інформації від витоку технічними каналами, проводити обслуговування і контроль стану апаратних засобів захисту інформації та комплексів технічною захисту інформації.

РН 21. Виконувати впровадження, підтримку, аналіз ефективності систем виявлення несанкціонованого доступу, дій з інформацією в інформаційній системі, вразливостей, можливих загроз інформаційному простору й інформаційним ресурсам та використовувати комплекси захисту для забезпечення необхідного рівня захищеності інформації в інформаційних системах.

РН 22. Вміти застосовувати методи та інструменти проєктування й адміністрування мереж і систем, виконувати налаштування, моніторинг та підтримку їхньої працездатності з урахуванням вимог інформаційної безпеки.

Заплановані результати навчання за навчальною дисципліною

Знання:

1. Принципи побудови КСЗІ в інформаційних та ІКС.
2. Нормативно-правову базу України у сфері кібербезпеки та захисту інформації, включаючи закони України, нормативні документи технічного захисту інформацій та міжнародні стандарти.
3. Типи загроз інформаційній безпеці, включаючи загрози створення технічних каналів витоку інформації.
4. Впровадження та супроводу КСЗІ в інформаційних та ІКС.
5. Архітектуру та принципи функціонування систем виявлення несанкціонованого доступу.
6. Модель загроз для інформації в ІКС.
7. Модель порушника безпеки інформації.
8. Методи криптографічного та технічного захисту інформації, включаючи засоби контролю доступу.
9. Процедури впровадження, налаштування, супроводу комплексів захисту інформації.

Уміння:

8. Застосовувати законодавство України та міжнародні стандарти для визначення вимог до КСЗІ під час здійснення професійної діяльності.
9. Обирати та застосовувати методи і засоби захисту інформації в ІКС відповідно до встановленої політики інформаційної безпеки організації.
10. Впроваджувати, налаштовувати та підтримувати функціонування програмних комплексів захисту інформації.
11. Визначати загрози НСД і створення технічних каналів витоку інформації на об’єктах інформаційної діяльності.
12. Використовувати комплекси захисту для забезпечення необхідного рівня захищеності інформації.
13. Виконувати моніторинг інформаційної безпеки.

Навички:

14. Розробка та впровадження КСЗІ в інформаційних системах різного призначення з урахуванням вимог нормативних документів.
15. Застосування методів криптографічного захисту для забезпечення конфіденційності, цілісності та доступності даних в ІКС.
16. Формування політик інформаційної безпеки та технічних завдань на створення (модернізацію) КСЗІ відповідно до вимог нормативні документи технічного захисту інформацій.
17. Адміністрування програмних комплексів захисту інформації.
18. Формування моделі загроз для інформації в ІКС відповідно до вимог нормативні документи технічного захисту інформацій.
19. Формування моделі порушника безпеки інформації.

3. ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Тема 1. Нормативно-правове забезпечення захисту інформації

Правові основи захисту інформації в Україні. Закони України «Про захист інформації в інформаційно-комунікаційних системах», «Про основні засади забезпечення кібербезпеки України» «Про інформацію», «Про захист персональних даних» та інші. Система нормативних документів технічного захисту інформації (НД ТЗІ). Структура та вимоги НД ТЗІ 3.7-003-2023. Міжнародні стандарти (ISO/IEC, NIST) та їх імплементація в українське законодавство. Відповідальність за порушення вимог законодавства у сфері захисту інформації.

Тема 2. Етапи створення КСЗІ. Порядок проведення робіт із створення КСЗІ в ІКС. Формування вимог до КСЗІ

Загальна структура та етапи створення комплексної системи захисту інформації (КСЗІ) згідно з НД ТЗІ 3.7-003-2023. Ініціювання створення КСЗІ: підстави та організаційні заходи. Формування вихідних вимог до КСЗІ залежно від категорії інформаційно-комунікаційної системи (ІКС) та виду інформації, що обробляється. Визначення відповідальних осіб та робочої групи. Попереднє визначення складу заходів захисту.

Тема 3. Обґрунтування необхідності створення КСЗІ. Категоріювання ІКС.

Аналіз потреби у створенні КСЗІ. Критерії віднесення ІКС до категорій: тип інформації, що обробляється (з обмеженим доступом, службова, критична), масштаб системи, кількість користувачів, наявність підключення до публічних мереж. Порядок проведення категоріювання ІКС. Оформлення результатів категоріювання. Визначення необхідного рівня захищеності інформації залежно від категорії ІКС.

Тема 4. Обстеження середовищ функціонування ІКС. Опис моделі порушника політики безпеки інформації. Опис моделі загроз для інформації.

Проведення обстеження ІКС: аналіз апаратного та програмного забезпечення, топології мережі, технологій обробки інформації, фізичного середовища функціонування. Визначення потенційних вразливостей. Формування моделі порушника: категорії порушників (зовнішні/внутрішні, рівень доступу, кваліфікація, мотивація, можливості), опис типових дій порушника. Формування моделі загроз для інформації: джерела загроз, актуальні загрози (НСД, витік технічними каналами, порушення цілісності/доступності), класифікація загроз згідно з методиками ТЗІ. Документальне оформлення результатів.

Тема 5. Формування завдання на створення КСЗІ. Розробка політики безпеки інформації в ІКС.

Структура та зміст завдання на створення КСЗІ. Визначення цілей, завдань та об’єктів захисту. Розробка політики безпеки інформації (ПБІ): мета, сфера дії, принципи забезпечення безпеки. Основні напрями політики: управління доступом, реєстрація та облік подій, захист від загроз, криптографічний захист, безпека мережевої взаємодії, управління інцидентами. Визначення організаційно-розпорядчих документів, що забезпечують реалізацію ПБІ.

Тема 6. Розробка технічного завдання на створення КСЗІ. Розробка проекту КСЗІ

Структура та зміст технічного завдання (ТЗ) на створення КСЗІ згідно з НД ТЗІ 3.7-003, НД ТЗІ 3.7-001: склад, зміст, порядок погодження та затвердження. Розробка проекту КСЗІ: вибір конкретних засобів захисту інформації (програмних, програмно-апаратних, організаційних). Проектна документація: пояснювальна записка, схеми розміщення засобів захисту, відомості обладнання, інструкції з експлуатації. Заходи із захисту інформації від витоку технічними каналами. Визначення порядку взаємодії засобів захисту між собою та з інфраструктурою ІКС.

Тема 7. Введення КСЗІ в дію та оцінка захищеності інформації в ІКС. Супровід КСЗІ

Порядок введення КСЗІ в дію: монтаж, налагодження, пусконалагоджувальні роботи. Проведення попередніх випробувань. Проведення державної експертизи та приймальних випробувань. Оцінка захищеності інформації в ІКС: методика проведення, критерії оцінки, оформлення результатів (висновок про захищеність). Введення КСЗІ в постійну експлуатацію. Супровід КСЗІ: моніторинг функціонування, періодичний контроль стану захисту (контрольні перевірки), управління змінами (оновлення, модернізація), реагування на інциденти, архівування журналів подій, забезпечення безперервності функціонування засобів захисту. Порядок виведення КСЗІ з експлуатації.

4. СТРУКТУРА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Назви змістових модулів і тем	Кількість годин									
	Денна форма					Заочна форма				
	усього	у тому числі				усього	у тому числі			
		лекц.	лаб.	прак.	сам. роб.		лекц.	лаб.	прак.	сам. роб.
Тема 1. Нормативно-правове забезпечення захисту інформації	18	2	2	2	12	20	2			18
Тема 2. Етапи створення КСЗІ. Порядок проведення робіт із створення КСЗІ в ІКС. Формування вимог до КСЗІ	20	4	2	2	12	22			2	20
Тема 3. Обґрунтування необхідності створення КСЗІ. Категоріювання ІКС	24	4	4	2	14	22		2		20
Тема 4. Обстеження середовищ функціонування ІКС. Опис моделі порушника політики безпеки інформації. Опис моделі загроз для інформації	20	4	2	2	12	22	2			20
Тема 5. Формування завдання на створення КСЗІ. Розробка політики безпеки інформації в ІКС	22	4	2	2	14	22		2		20
Тема 6. Розробка технічного завдання на створення КСЗІ. Розробка проекту КСЗІ	22	4	4	2	12	20				20
Тема 7. Введення КСЗІ в дію та оцінка захищеності інформації в ІКС. Супровід КСЗІ	24	4	4	2	14	22	2			20
Усього годин	**150**	**26**	**20**	**14**	**90**	**150**	**6**	**4**	**2**	**138**
ПІДСУМКОВИЙ КОНТРОЛЬ – ЕКЗАМЕН										

5. ПРАКТИЧНІ РОБОТИ

Назва теми	Кількість годин	
	Денна форма	Заочна форма
Тема 1. Нормативно-правові акти України щодо створення КСЗІ 1.1 Закону України “Про інформацію” 1.2 Закон України “Про захист персональних даних” 1.3 Закон України “Про захист інформації в інформаційно-комунікаційних системах” 1.4 НД ТЗІ 1.1-003-99 1.5 Концепції технічного захисту інформації в Україні	2	
Тема 2. Організація робіт служби захисту інформації 2.1 Положення про службу захисту інформації в ІКС 2.2 Функції СЗІ під час створення комплексної системи захисту інформації 2.3 Функції СЗІ під час експлуатації комплексної системи захисту інформації 2.4 Функції СЗІ з організації навчання персоналу з питань забезпечення захисту інформації	2	2
Тема 3. Міжнародний стандарт ISO/IEC 15408 3.1 Призначення стандарту ISO/IEC 15408 3.2 Структура вимог стандарту 3.3 Процес розроблення та кваліфікаційного аналізу 3.4 Загальна методологія оцінювання 3.5 Структури профілю захисту і завдання з безпеки	2	
Тема 4. Критерії захищеності інформації в комп’ютерних системах від несанкціонованого доступу 4.1 Критерії конфіденційності 4.2 Критерії доступності 4.3 Критерії цілісності	2	

Тема 5. Класифікація автоматизованих систем і стандартні функціональні профілі 5.1 Критерії спостереженості 5.2 Критерії гарантій 5.3 Класифікація автоматизованих систем 5.4 Функціональні профілі захищеності інформації	2	
Тема 6. Політики безпеки інформації в ІКС 3.1 Завдання захисту інформації в АС. 3.2 Класифікація інформації, що обробляється в АС. 3.3 Опис компонентів АС та технології обробки інформації. 3.4 Політика безпеки інформації в АС.	2	
Тема 7. Календарний план робіт з захисту інформації 7.1 Організаційні заходи 7.2 Контрольно-правові заходи 7.3 Профілактичні заходи 7.4 Інженерно-технічні заходи	2	
Всього	**14**	**2**

6. ЛАБОРАТОРНІ РОБОТИ

Назва теми	**Кількість годин**	
	Денна форма	**Заочна форма**
Тема 1. Розрахунок оцінки захищеності 1.1 Об'єктів інформаційної системи 1.2 Процесів і програм інформаційної системи 1.3 Каналу зв'язку інформаційної системи	2	2
Тема 2. Розрахунок оцінки захищеності 2.1 Витоку технічними каналами 2.2 Управління і контроль	2	
Тема 3. Розрахунок оцінки захищеності елементів системи захисту 3.1 Узагальнених кількісних оцінок профілю безпеки 3.2 Розрахунок кількісних і якісних оцінок рівня захищеності	2	
Тема 4. Створення та налаштування віртуальної машини VirtualBox 4.1 Завантаження образу VirtualBox 4.2 Встановлення VirtualBox 4.3 Налаштування VirtualBox	2	
Тема 5. Конфігурування параметрів безпеки операційної системи Windows на VirtualBox 5.1 Налаштування параметрів безпеки в операційної системи Windows	2	
Тема 6. Інсталяція системи ЛОЗА-1 на VirtualBox 6.1 Модернізація та відновлення компонентів системи	2	
Тема 7. Адміністрування системи ЛОЗА-1 на VirtualBox 7.1 Експлуатація програмних засобів, призначених для адміністрування системи ЛОЗА-1 програма *Аудитор*	2	
Тема 8. Адміністрування системи ЛОЗА-1 на VirtualBox 8.1 Експлуатація програмних засобів, призначених для адміністрування системи ЛОЗА-1 програма *Керування захистом, Монітор захисту*	2	
Тема 9. Дослідження та визначення функціональних профілів захисту 9.1 Визначення клас АС згідно з НД ТЗІ 2.5-005 9.2 Складання та опис функціонального профілю захищеності визначеного класу 9.3 Розробка організаційно-технічних заходів захисту	2	2
Тема 10. Дослідження проведення експертних випробувань 10.1 Програми та методики випробувань. Атестація відповідності КСЗІ	2	
Всього	**20**	**4**

7. САМОСТІЙНА РОБОТА

До самостійної роботи студентів щодо вивчення дисципліни «Комплексні системи захисту інформації» включаються:

1. Знайомство з науковою та навчальною літературою відповідно зазначених у програмі тем.
2. Опрацювання лекційного матеріалу.
3. Підготовка до практичних занять.
4. Консультації з викладачем протягом семестру.
5. Самостійне опрацювання окремих питань навчальної дисципліни.
6. Підготовка та виконання контрольних робіт.
7. Підготовка до підсумкового контролю.

Тематика та питання до самостійної підготовки та індивідуальних завдань

№ з/п	Назва теми	Кількість годин	
		денна форма	заочна форма
1	**Тема 1. Системний підхід до побудови комплексних систем захисту інформації.** Поняття комплексної системи захисту інформації (КСЗІ), як об'єкта проєктування. Принципи побудови КСЗІ (комплексність, безперервність, своєчасність). Життєвий цикл КСЗІ. Взаємозв'язок організаційних, технічних та програмних заходів.	12	18
2	**Тема 2. Нормативно-правове регулювання захисту інформації.** Законодавча база України у сфері КСЗІ. Порядок категоріювання об'єктів інформаційної діяльності (НД ТЗІ 1.6-005-2013). Вимоги до захисту інформації залежно від категорії об'єкта. Державна експертиза КСЗІ.	12	20
3	**Тема 3. Моделювання загроз та оцінка ризиків у КСЗІ.** Розробка моделі загроз для об'єкта інформаційної діяльності. Методики кількісної та якісної оцінки ризиків. Визначення актуальних загроз та вразливостей. Обґрунтування необхідності створення КСЗІ.	14	20
4	**Тема 4. Політика безпеки та організаційні заходи захисту.** Розробка політики інформаційної безпеки організації. Організаційна структура служби захисту інформації. Режимні заходи та робота з персоналом. Інструкції та регламенти з безпеки. Обстеження середовищ функціонування ІКС, моделі порушника, моделі загроз.	12	20
5	Тема **5. Проєктування КСЗІ: технічне завдання та обґрунтування.** Порядок розробки технічного завдання на створення КСЗІ (НД ТЗІ 1.6-005-2013). Вибір засобів захисту та їх обґрунтування. Профіль захисту та функціональні вимоги безпеки. Етапи проєктування системи.	14	20
6	**Тема 6. Впровадження, введення в дію та атестація КСЗІ.** Порядок проведення робіт із створення КСЗІ (НД ТЗІ 3.7-003-2023). Процедури введення системи в промислову експлуатацію. Атестація робочих місць та системи в цілому. Оформлення експлуатаційної документації.	12	20
7	**Тема 7. Експлуатація, аудит та оцінка ефективності КСЗІ.** Організація супроводу КСЗІ. Моніторинг інформаційних процесів та реагування на інциденти. Методи оцінки ефективності функціонування КСЗІ. Проведення аудиту безпеки та інтерпретація результатів.	14	20
	Всього	**90**	**138**

8. ВИДИ ТА МЕТОДИ КОНТРОЛЮ

Види контролю	Складові оцінювання	
	Для екзамену	Для заліку
поточний контроль, який здійснюється у ході: проведення практичних (лабораторних) занять, виконання самостійної роботи, індивідуальних завдань, дослідна робота здобувача тощо.	**50%**	**100%**
підсумковий контроль	**50%**	

Методи діагностики знань (контролю)	фронтальне опитування; наукова доповідь, реферати, усне повідомлення, індивідуальне опитування; робота у групах; ділова гра, розв`язання ситуаційних завдань, кейсів, практичних завдань, екзамен

Питання до екзамену

Тема 1. Нормативно-правове забезпечення захисту інформації

Правові основи захисту інформації в Україні: система законодавства у сфері захисту інформації та кібербезпеки.

Закон України «Про захист інформації в інформаційно-комунікаційних системах»: сфера дії, основні положення, права та обов'язки суб'єктів.

Закон України «Про основні засади забезпечення кібербезпеки України»: мета, суб'єкти забезпечення кібербезпеки, основні завдання.

Закон України «Про інформацію»: поняття інформації, види інформації, правовий режим доступу до інформації.

Закон України «Про захист персональних даних»: визначення персональних даних, вимоги до обробки та захисту, права суб'єктів персональних даних.

Система нормативних документів технічного захисту інформації (НД ТЗІ): структура, класифікація, призначення, порядок затвердження.

НД ТЗІ 3.7-003-2023 «Захист інформації в інформаційно-комунікаційних системах. Загальні положення»: структура, основні вимоги, сфера застосування.

Міжнародні стандарти у сфері захисту інформації: структура, принципи, імплементація в українське законодавство.

Тема 2. Етапи створення КСЗІ. Порядок проведення робіт із створення КСЗІ в ІКС. Формування вимог до КСЗІ

Загальна структура та етапи створення комплексної системи захисту інформації (КСЗІ) згідно з НД ТЗІ 3.7-003-2023.

Ініціювання створення КСЗІ: підстави для створення, організаційні заходи.

Формування служби захисту інформації зі створення КСЗІ: склад, функції, права та обов'язки членів робочої групи.

Формування вихідних вимог до КСЗІ: фактори, що впливають на вимоги (категорія ІКС, вид інформації, технології обробки).

Структура та зміст вихідних вимог до КСЗІ: основні напрями захисту, вимоги до управління доступом, реєстрації подій, захисту від НСД.

Попереднє визначення складу заходів захисту: організаційні, програмні, програмно-апаратні, криптографічні заходи.

Документальне оформлення рішення про створення КСЗІ: накази керівника, склад служби захисту інформації.

Функції служби захисту інформації під час створення та експлуатації комплексної системи захисту інформації.

Тема 3. Обґрунтування необхідності створення КСЗІ. Категоріювання ІКС

Аналіз потреби у створенні КСЗІ: методика обґрунтування, критерії необхідності створення.

Критерії віднесення інформаційно-комунікаційної системи (ІКС) до категорій: тип інформації, що обробляється (з обмеженим доступом, службова, критична, відкрита).

Порядок проведення категоріювання ІКС.

Оформлення результатів категоріювання ІКС: склад документів, форма висновку про категоріювання.

Обґрунтування необхідності створення комплексної системи захисту інформації.

Тема 4. Обстеження середовищ функціонування ІКС. Опис моделі порушника політики безпеки інформації. Опис моделі загроз для інформації

Проведення обстеження ІКС: мета, завдання, методи.

Аналіз апаратного та програмного забезпечення ІКС: перелік обладнання, програмних засобів, їх характеристик, вразливостей.

Аналіз топології мережі, технологій обробки інформації, фізичного середовища функціонування ІКС.

Визначення потенційних вразливостей ІКС: методика виявлення, класифікація вразливостей.

Формування моделі порушника безпеки інформації: категорії порушників (зовнішні/внутрішні), рівень доступу, кваліфікація, мотивація, можливості.

Опис типових дій порушника: методи та засоби реалізації загроз.

Формування моделі загроз для інформації: джерела загроз, актуальні загрози (НСД, витік технічними каналами, порушення цілісності/доступності).

Класифікація загроз згідно з методиками ТЗІ та документальне оформлення результатів обстеження, моделі порушника, моделі загроз.

Розробка політики безпеки інформації.

Розробка моделі порушника безпеки інформації.

Тема 5. Формування завдання на створення КСЗІ. Розробка політики безпеки інформації в ІКС

Структура та зміст завдання на створення КСЗІ: мета, завдання, об'єкти захисту.

Визначення цілей, завдань та об'єктів захисту при формуванні завдання на створення КСЗІ.

Розробка політики безпеки інформації: мета, сфера дії, принципи забезпечення безпеки.

Основні напрями політики безпеки інформації: управління доступом, реєстрація та облік подій, захист від загроз.

Основні напрями політики безпеки інформації.

Визначення організаційно-розпорядчих документів, що забезпечують реалізацію політики безпеки інформації.

Тема 6. Розробка технічного завдання на створення КСЗІ. Розробка проекту КСЗІ

Структура та зміст технічного завдання (ТЗ) на створення КСЗІ згідно з НД ТЗІ 3.7-003 та НД ТЗІ 3.7-001.

Порядок погодження та затвердження технічного завдання на створення КСЗІ.

Розробка проекту КСЗІ.

Склад проектної документації КСЗІ.

Заходи із захисту інформації від витоку технічними каналами в проекті КСЗІ.

Тема 7. Введення КСЗІ в дію та оцінка захищеності інформації в ІКС. Супровід КСЗІ

Порядок введення КСЗІ в дію: монтаж, налагодження, пусконалагоджувальні роботи.

Проведення попередніх випробувань КСЗІ: мета, завдання, порядок проведення, оформлення результатів.

Проведення державної експертизи КСЗІ: підстави, порядок проведення, результати.

Проведення приймальних випробувань КСЗІ: склад комісії, програма та методика випробувань, оформлення акта.

Оцінка захищеності інформації в ІКС: методика проведення, критерії оцінки.

Оформлення результатів оцінки захищеності: висновок про захищеність інформації в ІКС.

Введення КСЗІ в постійну експлуатацію: підстави, порядок, документальне оформлення.

Організація супроводу КСЗІ: призначення відповідальних, взаємодія з розробником, регламенти супроводу.

Атестація відповідності КСЗІ: мета, порядок проведення, атестат відповідності, строк дії, умови підтримання чинності.

9. ОЦІНЮВАННЯ ЗДОБУВАЧІВ ВИЩОЇ ТА ФАХОВОЇ ПЕРДВИЩОЇ ОСВІТИ ЗА НАВЧАЛЬНУ ДИСЦИПЛІНУ У МІЖНАРОДНОМУ ГУМАНІТАРНОМУ УНІВЕРСИТЕТІ

(*поточний контроль, підсумковий контроль, загальний результат оцінювання)*

ЕКЗАМЕН

Поточний контроль			
Види роботи	**Планові терміни виконання**	**Форми контролю та звітності**	**Максимальний відсоток оцінювання**
Систематичність і активність роботи на практичних (лабораторних) заняттях			
1.1. Підготовка до практичних (лабораторних) занять	Відповідно до робочої програми та розкладу занять	Перевірка обсягу та якості засвоєного матеріалу під час практичних (лабораторних) занять	**30**
Виконання завдань для самостійного опрацювання			
1.2. Індивідуальне тестування, завдання, підготовка реферату (есе) за заданою тематикою	Відповідно до робочої програми тарозкладу занять	Розгляд відповідного матеріалу під час аудиторних занять або ІКР, перевірка конспектів навчальних текстів тощо	**10**
Виконання індивідуальних завдань, дослідна робота здобувача			
1.3. Інші види індивідуальних завдань, в т.ч. підготовка наукових публікацій, участь у роботі круглих столів, конференцій тощо.	Відповідно до робочої програми тарозкладу занять	Обговорення результатів проведеної роботи під час аудиторних занять, наукових конференцій та круглих столів.	**10**
Разом балів за поточний контроль			**50**
Підсумковий контроль **екзамен**			**50**
Загальний результат оцінювання			**100**

Поточний контроль знань здобувачів освіти при формі контролю **екзамен** (максимум 50 балів) оцінюється за шкалою *(«2», «3», «4», «5»)*, з обов'язковим переведенням балів за кожний вид роботи таким чином:

- за підготовку до аудиторних занять (максимум 30 балів) здобувачу освіти необхідно мати не менше 1/2 оцінок від загальної кількості практичних (лабораторних) занять, для переводу балів за підготовку до аудиторних занять середньоарифметична оцінка множиться на коефіцієнт 6;
- за виконання завдань для самостійного опрацювання (тестування, завдання, підготовка реферату (есе) за заданою тематикою) (максимум 10 балів) здобувачу освіти необхідно мати не менше 1/2 оцінок від загальної кількості програмного матеріалу, що виноситься на самостійне вивчення, для переводу зазначених балів середньоарифметична оцінка множиться на коефіцієнт 2;
- за інші види індивідуальних завдань, в т.ч. підготовку наукових публікацій, участь у роботі круглих столів, конференцій тощо (максимум 10- балів) здобувачу освіти необхідно мати не менше 1/2 оцінок від загальної кількості інших видів індивідуальних завдань, для переводу балів за підготовку до аудиторних занять середньоарифметична оцінка множиться на коефіцієнт 2.

КРИТЕРІЇ ОЦІНЮВАННЯ ЗА ПОТОЧНИЙ КОНТРОЛЬ

- «2»- виставляється за неправильну відповідь (письмову роботу), яка не відповідає змісту теми та свідчить про нерозуміння її основних положень;
- «3» -виставляється за відповідь (письмову роботу), яка відповідає змісту теми, але є неповною і неточною у визначенні понять, свідчить про неповне розуміння основних положень навчального матеріалу, свідчить про те, що знання студента мають фрагментарний, поверховий характер;
- «4» - оцінюється правильна і обґрунтована відповідь (письмова робота), з якої видно, що студент знає й розуміє теоретичний матеріал в обсязі навчальної теми, володіє необхідними навичками, не допускає суттєвих помилок.
- «5» - оцінюється повна, правильна, ґрунтовна відповідь (письмова робота) на запитання теми, що передбачає логічність і послідовність викладу матеріалу, володіння термінологією, показує вміння повно й глибоко використовувати теоретичні знання в практичній площині.

КРИТЕРІЇ ОЦІНЮВАННЯ ПІДСУМКОВОГО КОНТРОЛЮ ЗНАНЬ ЗДОБУВАЧІВ ЗА ІСПИТ (максимум 50 балів)

Рівень знань оцінюється:

- від 40 до 50 балів - студент виявляє особливі творчі здібності, вміє самостійно знаходити та опрацьовувати необхідну інформацію, демонструє знання матеріалу, проводить узагальнення і висновки;
- 30 до 40 балів - студент володіє знаннями матеріалу, але допускає незначні помилки у формуванні термінів, категорій, проте за допомогою викладача швидко орієнтується і знаходить правильні відповіді;
- 20 - 30 балів - студент відтворює значну частину теоретичного матеріалу, виявляє знання і розуміння основних положень, з допомогою викладача може аналізувати навчальний матеріал, але дає недостатньо обґрунтовані, невичерпні відповіді, допускає помилки.
- 10 - 20 балів - володіє навчальним матеріалом на середньому рівні, допускає помилки, серед яких є значна кількість суттєвих;
- 0 10 балів - володіє навчальним матеріалом на рівні, вищому за початковий, значну частину його відтворює на репродуктивному рівні, на всі запитання дає необґрунтовані, невичерпні відповіді, допускає помилки.

10. КРИТЕРІЇ ЗАГАЛЬНИХ РЕЗУЛЬТАТІВ ОЦІНЮВАННЯ ЗНАНЬ ЗДОБУВАЧІВ (для іспиту / заліку)

Рівень знань оцінюється:

- «відмінно» / «зараховано» A - від 90 до 100 балів. Студент виявляє особливі творчі здібності, вміє самостійно знаходити та опрацьовувати необхідну інформацію, демонструє знання матеріалу, проводить узагальнення і висновки. Був присутній на лекціях та семінарських заняттях, під час яких давав вичерпні, обґрунтовані, теоретично і практично правильні відповіді, має конспект з виконаними завданнями до самостійної роботи, презентував реферат (есе) за заданою тематикою, проявляє активність і творчість у науково-дослідній роботі;
- «добре» / «зараховано» B - від 82 до 89 балів. Студент володіє знаннями матеріалу, але допускає незначні помилки у формуванні термінів, категорій, проте за допомогою викладача швидко орієнтується і знаходить правильні відповіді. Був присутній на лекціях та семінарських заняттях, має конспект з виконаними завданнями до самостійної роботи, презентував реферат (есе) за заданою тематикою, проявляє активність і творчість у науково-дослідній роботі;
- «добре» / «зараховано» C - від 74 до 81 балів. Студент відтворює значну частину теоретичного матеріалу, виявляє знання і розуміння основних положень, з допомогою викладача може аналізувати навчальний матеріал, але дає недостатньо обґрунтовані, невичерпні відповіді, допускає помилки. При цьому враховується наявність конспекту з виконаними завданнями до самостійної роботи, реферату та активність у науково-дослідній роботі;
- «задовільно» / «зараховано» D - від 64 до 73 балів. Студент був присутній не на всіх лекціях та семінарських заняттях, володіє навчальним матеріалом на середньому рівні, допускає помилки, серед яких є значна кількість суттєвих. При цьому враховується наявність конспекту з

виконаними завданнями до самостійної роботи, рефератів (есе);

- «задовільно» / «зараховано» E - від 60 до 63 балів. Студент був присутній не на всіх лекціях та семінарських заняттях, володіє навчальним матеріалом на рівні, вищому за початковий, значну частину його відтворює на репродуктивному рівні, на всі запитання дає необґрунтовані, невичерпні відповіді, допускає помилки, має неповний конспект з завданнями до самостійної роботи.
- «незадовільно з можливістю повторного складання» / «не зараховано» FX – від 35 до 59 балів. Студент володіє матеріалом на рівні окремих фрагментів, що становлять незначну частину навчального матеріалу.
- «незадовільно з обов'язковим повторним вивченням дисципліни» / «не зараховано» F – від 0 до 34 балів. Студент не володіє навчальним матеріалом.

ТАБЛИЦЯ ВІДПОВІДНОСТІ ЗАГАЛЬНИХ РЕЗУЛЬТАТІВ ОЦІНЮВАННЯ ЗНАНЬ ЗА РІЗНИМИ ШКАЛАМИ

100-бальною шкалою	Шкала за ECTS	За національною шкалою	
		екзамен	залік
90-100	A	Відмінно	Зараховано
82-89	B	Добре	
74-81	C		
64-73	D	Задовільно	
60-63	E		
35-59	FX	Незадовільно	Не зараховано
1-34	F		

11. РЕКОМЕНДОВАНА ЛІТЕРАТУРА

Основна

1. Про внесення змін до Закону України "Про інформацію" № 2938-VI від 13.01.2011. – Відомості Верховної Ради України 2011, № 32, ст. 313.
2. Закон України "Про захист персональних даних" № 2297-VI від 01.06.2010. – Відомості Верховної Ради України 2010, № 34, ст. 481.
3. Закон України "Про критичну інфраструктуру" № 2684-IX від 18.10.2022.
4. Онацький О.В., Йона Л.Г., Бєлова Ю.В. Криптографічний захист інформації: Навч. посібник. - Одеса: Одеса : «Астропринт» 2023. 252с. https://surl.li/onvhbl
5. Йона Л.Г., Онацький О.В., Швець О.В. Системи банківської безпеки: Навч. посібник.- Одеса: ДУІТЗ. 2022. 192с. https://surl.lt/hpdpub
6. Онацький О.В. Методологія створення комплексної системи захисту інформації / Прикладная радиоэлектроника: науч.-техн. журнал ХНУР – 2014. Том 13. – № 3 – С. 350-356.
7. Онацький О. В., Йона Л. Г. Криптографічні системи : навчальний посібник з дисциплін "Криптографія та криптоаналіз" для освітньо-професійної підготовки бакалаврів в галузі знань 12 "Інформаційні технології" за спеціальністю 125 "Кібербезпека" / О. В. Онацький, Л. Г. Йона. – Одеса : Міжнародний гуманітарний університет, 2023. – 156 с. https://surl.li/oqiqhk
8. НД ТЗІ 3.7-003-2023 Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-комунікаційній системі (Наказ Адміністрації Держспецзв'язку від 28.10.2023 № 924).
9. НД ТЗІ 2.5-004. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу. – Затверджено наказом ДСТСЗІ СБ України № 22.

10. НД ТЗІ 2.5-005. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу. – Затверджено наказом ДСТСЗІ СБ України № 22.

11. Положення про Державну експертизу в сфері технічного захисту інформації. – Затверджено наказом Адміністрації ДССЗЗІ України № 93 від 16.05.07.

12. НД ТЗІ 2.6-001-11. Порядок проведення робіт з державної експертизи засобів технічного захисту інформації від несанкціонованого доступу та комплексних систем захисту інформації в інформаційно-телекомунікаційних системах. – Затверджено наказом Адміністрації ДССЗЗІ України № 65 від 12 березня 2011.

13. НД ТЗІ 3.6-004-21 Порядок впровадження системи безпеки інформації в державних органах, на підприємствах, організаціях, в інформаційно-комунікаційних системах яких обробляється інформація, вимога щодо захисту якої встановлена законом та не становить державної таємниці.

14. НД ТЗІ 2.3-025-21 Методика оцінювання заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, затверджений наказом Адміністрації Держспецзв'язку від 01.02.2022 року № 53.

15. НД ТЗІ 3.6-005-21 Порядок категоріювання безпеки інформаційної системи та інформації.

16. НД ТЗІ 2.6-004-21 Порядок авторизації безпеки інформаційних систем.

17. НД ТЗІ 3.6-008-21 Порядок моніторингу безпеки інформаційних систем.

Допоміжна

18. ДСТУ ISO/IEC 27002:2015 Інформаційні технології. Методи захисту. Звід практик щодо заходів інформаційної безпеки.

19. ДСТУ 3396.1. Захист інформації. Технічний захист інформації. Порядок проведення робіт.

20. 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.

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

22. Про внесення змін до Закону України "Про захист інформації в автоматизованих системах" № 2594-IV від 31.05.2005. – Відомості Верховної Ради України 2005, № 26, ст. 347.

23. Домарєв В.В., Скворцов С.О. Організація захисту інформації на об'єктах державної та підприємницької діяльності. Навчальний посібник. – К.: Вид-во Європ. Ун-ту, 2006. – 102 с.

24. Онацький О.В. Методологія створення комплексної системі захисту інформацій / 68-ма науково-технічна конференція професорсько-викладацького складу, науковців, молодих вчених, аспірантів та студентів. Частина ІІІ. Одеса 4-6 груд. – 2013.– С. 152-155.

25. Онацький О.В. Аналіз стандартів інформаційної безпеки. Матеріали 71-ої науково-технічної конференції професорсько-викладацького складу, науковців, молодих вчених, аспірантів та студентів ОНАЗ ім. О.С. Попова. Частина І. Одеса 6-8 грудня. – 2016. – С. 71 – 74.

26. Онацький О.В. Аналіз програмних і технічних засобів захисту інформації. Матеріали 72-га науково-технічної конференції професорсько-викладацького складу, науковців, молодих вчених, аспірантів та студентів ОНАЗ ім. О.С. Попова. Частина І. Одеса 13-15 грудня. – 2017. – С. 135 – 137.

27. Онацький О.В. Аналіз системи виявлення вторгнень. Матеріали 72-га науково-технічної конференції професорсько-викладацького складу, науковців, молодих вчених, аспірантів та студентів ОНАЗ ім. О.С. Попова. Частина І. Одеса 13-15 грудня. – 2017. – С. 106 – 107.

28. Онацький О.В. Створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі. Матеріали 72-га науково-технічної конференції професорсько-викладацького складу, науковців, молодих вчених, аспірантів та студентів ОНАЗ ім. О.С. Попова. Частина І. Одеса 13-15 грудня. – 2017. – С. 152 – 154.

29. Онацький О.В. Щодо питань захисту інформаційних ресурсів медичних підприємств. Матеріали 75-а науково-технічної конференції професорсько-викладацького складу, науковців,

молодих вчених, аспірантів та студентів ОНАЗ ім. О.С. Попова. Частина І. Одеса 11-15 грудня. – 2020. – С. 122 – 124.

30. Онацький О.В. Аналіз комплексів засобів захисту від несанкціонованого доступу на базі операційної системи. 73-я науково-технічна конференція професорсько-викладацького складу, науковців, аспірантів та студентів ОНАЗ ім. О.С. Попова 12-14 грудня 2018 р. – С. 145 – 146.

31. Онацький О.В. Аналіз та розробка методики управління інцидентами у сфері інформаційної безпеки підприємства. 76-й Науково-технічній конференції професорсько-викладацького складу, науковців, аспірантів та студентів**.** Одеса 15-16 грудня. – 2021 р.

Інформаційні ресурси

32. Сайт Державної служби спеціального зв'язку та захисту інформації. URL: https://cip.gov.ua/ua

33. Сайт Технічний захист інформації. URL: https://tzi.ua/ua/index.html

34. Комплексні системи захисту інформації. URL: https://web.posibnyky.vntu.edu.ua/fmib/41yaremchuk_kompleksni_systemy_zahystu_informaciyi/

35. Комплексні системи захисту інформації. Проектування, впровадження, супровід. URL: https://books.google.com.ua/books?id=GcBlDwAAQBAJ&printsec=frontcover&hl=ru&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false

36. Сайт Computer Emergency Response Team of Ukraine. URL: https://cert.gov.ua

37. https://zakon.rada.gov.ua/laws