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

СИСТЕМИ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

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

Одеса - 2025 рік

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

Розробники і викладачі	**Контактний тел.**	**E-mail**
професор кафедри комп'ютерної інженерії та інноваційних технологій, д.т.н., професор **Соколов Артем Вікторович, к.т.н. Йона Лариса Григорівна**	050-492-32-57	radiosquid@gmail.com

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

1. 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="2">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>5-й</td><td>5-й</td></tr>
<tr><td colspan="2">Лекції</td></tr>
<tr><td rowspan="9">Мова навчання – українська</td><td rowspan="9">Рівень вищої освіти – перший (бакалаврський) рівень</td><td>26 год.</td><td>6 год.</td></tr>
<tr><td colspan="2">Практичні, семінарські</td></tr>
<tr><td>20 год.</td><td>4 год.</td></tr>
<tr><td colspan="2">Лабораторні</td></tr>
<tr><td>6 год.</td><td>2 год.</td></tr>
<tr><td colspan="2">Самостійна робота та індивідуальні завдання</td></tr>
<tr><td>98 год.</td><td>138 год.</td></tr>
<tr><td colspan="2">Вид контролю:</td></tr>
<tr><td>екзамен</td><td>екзамен</td></tr>
</table>

Дисципліна «Системи технічного захисту інформації» є обов'язковою складовою освітньо-професійної програми підготовки бакалаврів зі спеціальності 125 «Кібербезпека та захист інформації» та спрямована на формування у здобувачів системних знань і практичних навичок щодо виявлення, аналізу та нейтралізації технічних каналів витоку інформації. Дисципліна охоплює фізичні основи виникнення загроз витоку, класифікацію технічних каналів (акустичні, електромагнітні, оптичні, віброакустичні), методи та засоби захисту від несанкціонованого зняття інформації, апаратні комплекси контролю доступу, а також методики технічного інспектування та контролю захищеності об'єктів.

Метою викладання дисципліни є забезпечення здобувачів фундаментальними знаннями з принципів функціонування технічних каналів витоку інформації, механізмів екранування, фільтрації та ізоляції, а також набуття практичних умінь застосовувати спеціалізовані засоби технічного захисту, проводити спеціальні перевірки приміщень, оцінювати ефективність заходів ТЗІ та оформлювати результати технічного контролю відповідно до вимог нормативних документів України у сфері технічного захисту інформації.

ПРЕРЕКВІЗИТИ. Передумовами для вивчення дисципліни є знання з фізики (ОК 7), теорії інформації та кодування (ОК 25), цифрової обробки сигналів (ОК 17), криптографії та криптоаналізу (ОК 23), а також «Захисту інформації в інфокомунікаційних системах та мережах» (ОК 12).

ПОСТРЕКВІЗИТИ. Знання методів і засобів технічного захисту інформації є важливими при вивченні «Комплексних систем захисту інформації» (ОК 24), «Управління інформаційною та кібербезпекою» (ОК 30), «Безпеки бездротових мереж Інтернету речей (IoT)» (ОК 27) та «Етичного хакінгу та тестування на проникнення» (ОК 18), а також при підготовці кваліфікаційної роботи (ОК 36).

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

У процесі реалізації програми дисципліни «Етичний хакінг та тестування на проникнення» формуються наступні компетентності із передбачених освітньою програмою:

Інтегральна компетентність

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

Загальні компетентності (ЗК)

ЗК1. Здатність застосовувати знання у практичних ситуаціях.

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

Спеціальні (фахові, предметні) компетентності

СК 1. Здатність застосовувати законодавчу та нормативно правову базу, а також державні та міжнародні вимоги, практики і стандарти у професійній діяльності

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 «Системи технічного захисту інформації» забезпечує досягнення програмних результатів навчання (РН), передбачених освітньою програмою:

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 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:

- основні принципи та методи технічного захисту інформації;
- класифікацію загроз інформаційній безпеці та відповідні технічні засоби протидії;
- архітектуру систем технічного захисту та їх взаємодію з організаційними та програмними засобами;
- нормативно-правові акти та міжнародні стандарти у сфері технічного захисту інформації;
- методи контролю ефективності та сертифікації систем захисту;

Уміння:

- аналізувати загрози та оцінювати ризики для інформаційних систем;
- проектувати та обґрунтовувати структуру системи технічного захисту для конкретних

умов;
- застосовувати апаратні та програмно-апаратні засоби захисту (системи контролю доступу, криптографічні модулі, засоби екранування тощо);
- проводити тестування та аудит ефективності технічних засобів захисту;
- інтегрувати системи технічного захисту у комплексну систему інформаційної безпеки організації;
- документувати результати аналізу, проектування та впровадження систем захисту відповідно до стандартів.

3. ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Тема 1. Основи технічного захисту інформації та канали витоку. Поняття та завдання технічного захисту інформації. Класифікація каналів витоку інформації. Акустичні, електромагнітні, оптичні та інші канали. Нормативно-правова база та стандарти у сфері ТЗІ. Загальні методи протидії та інтеграція у комплексну систему безпеки.

Тема 2. Захист від витоку інформації акустичними та віброакустичними каналами. Характеристика акустичних та віброакустичних каналів. Методи перехоплення мовної інформації. Засоби акустичної ізоляції та звукопоглинання. Технічні системи активного та пасивного захисту. Практичні приклади та лабораторні методики.

Тема 3. Захист від витоку інформації електромагнітними та радіоканалами. Електромагнітні випромінювання як канал витоку. Радіотехнічні методи перехоплення. Екранування, заземлення та фільтрація сигналів. Стандарти TEMPEST та їх застосування. Прилади контролю та вимірювання рівня випромінювань.

Тема 4. Захист оптичних та візуальних каналів витоку інформації. Оптичні та візуальні канали витоку (спостереження, фото, відео). Методи прихованого знімання інформації. Технічні та організаційні засоби протидії. Використання світлофільтрів, штор, захисних екранів. Практичні приклади та аналіз інцидентів.

Тема 5. Апаратні засоби контролю доступу та фізичного захисту. Системи контролю та управління доступом (СКУД). Біометричні засоби ідентифікації. Замки, сейфи, охоронні сигналізації. Інтеграція фізичного захисту з інформаційними системами. Практичні аспекти впровадження.

Тема 6. Спеціалізовані технічні засоби та комплекси захисту. Комплекси технічного захисту інформації. Засоби виявлення несанкціонованих пристроїв перехоплення. Системи активного придушення каналів витоку. Інтегровані рішення для корпоративних та державних структур. Огляд сучасних технологій.

Тема 7. Технічний контроль та інспектування захищеності об'єктів. Поняття та завдання технічного контролю. Методи інспектування та аудиту захищеності. Використання вимірювальної апаратури. Документування результатів перевірок. Практика сертифікації та атестації об’єктів.

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.	практ.	сам. роб.		лекц.	лаб.	практ.	сам. роб.
Тема 1. Основи технічного захисту інформації та канали витоку.	18	2		2	14	22	2			20
Тема 2. Захист від витоку інформації акустичними та віброакустичними каналами.	22	4	2	2	14	20				20
Тема 3. Захист від витоку інформації електромагнітними та радіоканалами.	22	4		4	14	22		2		20
Тема 4. Захист оптичних та візуальних каналів витоку інформації.	22	4	2	2	14	22	2			20
Тема 5. Апаратні засоби контролю доступу та фізичного захисту.	22	4	2	2	14	22			2	20
Тема 6. Спеціалізовані технічні засоби та комплекси захисту.	22	4		4	14	20			2	18
Тема 7. Технічний контроль та інспектування захищеності об'єктів.	22	4		4	14	22	2			20
Усього годин	**150**	**26**	**6**	**20**	**98**	**150**	**6**	**2**	**4**	**138**
ПІДСУМКОВИЙ КОНТРОЛЬ – ЕКЗАМЕН										

5. ПРАКТИЧНІ РОБОТИ

№ з/п	Назва теми	Кількість годин	
		денна форма	заочна форма
1	**Тема 1. Основи технічного захисту інформації та канали витоку**. «Виявлення та класифікація каналів витоку інформації»	2	-
2	**Тема 2. Захист від витоку інформації акустичними та віброакустичними каналами.** «Дослідження акустичних каналів витоку»	2	-
3	**Тема 3. Захист від витоку інформації електромагнітними та радіоканалами.** «Вимірювання електромагнітних випромінювань обладнання». «Екранування та заземлення технічних засобів»	4	-
4	**Тема 4. Захист оптичних та візуальних каналів витоку інформації.** «Виявлення можливостей візуального спостереження»	2	-
5	**Тема 5. Апаратні засоби контролю доступу та фізичного захисту.** «Використання біометричних засобів ідентифікації»	2	2
6	**Тема 6. Спеціалізовані технічні засоби та комплекси захисту.** «Аналіз сучасних комплексів технічного захисту»	4	2
7	**Тема 7. Технічний контроль та інспектування захищеності об'єктів.** «Документування результатів технічного контролю».	4	-
	Всього	**20**	**4**

ТЕХНІЧНЕ Й ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ / ОБЛАДНАННЯ

Студенти отримують теми та питання курсу, основну і додаткову літературу, рекомендації, завдання та оцінки за їх виконання як традиційним шляхом, так і з використанням університетської платформи он-лайн навчання на базі Moodle. Окрім того, практичні навички у пошуку та аналізу інформації за курсом, з оформлення індивідуальних завдань, тощо, студенти отримують, користуючись університетськими комп'ютерними класами та бібліотекою.

5. ЛАБОРАТОРНІ РОБОТИ

№ з/п	Назва теми	Кількість годин	
		денна форма	заочна форма
1	**Тема 1. Основи технічного захисту інформації та канали витоку**.	-	
2	**Тема 2. Захист від витоку інформації акустичними та віброакустичними каналами.** «Моделювання витоку мовної інформації через вібраційні канали»	2	-
3	**Тема 3. Захист від витоку інформації електромагнітними та радіоканалами.**		
4	**Тема 4. Захист оптичних та візуальних каналів витоку інформації.** «Моделювання витоку інформації через оптичні канали»	2	2
5	**Тема 5. Апаратні засоби контролю доступу та фізичного захисту.** «Ознайомлення з роботою систем контролю доступу (СКУД)»	2	-
6	**Тема 6. Спеціалізовані технічні засоби та комплекси захисту.**	-	-
7	**Тема 7. Технічний контроль та інспектування захищеності об'єктів.**	-	-
	Всього	**6**	**2**

6. САМОСТІЙНА РОБОТА

До самостійної роботи студентів щодо вивчення дисципліни «Етичний хакінг та тестування на проникнення» 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 індивідуальних завдань.
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. Основи технічного захисту інформації та канали витоку. Поняття технічного захисту інформації (ТЗІ). Класифікація технічних каналів витоку інформації (акустичні, електромагнітні, оптичні, матеріально-речовинні). Фізичні основи виникнення загроз витоку. Нормативне забезпечення ТЗІ.	14	20
2	Тема 2. Захист від витоку інформації акустичними та віброакустичними каналами. Методи зниження чутливості приміщень. Засоби активної та пасивної звукоізоляції. Віброакустичні загрози та методи їх нейтралізації. Контроль акустичного фону.	14	20
3	Тема 3. Захист від витоку інформації електромагнітними та радіоканалами. Побічні електромагнітні випромінювання та наведення (ПЕМВН). Екранування приміщень та апаратури. Фільтрація мереж живлення та заземлення. Засоби радіоконтролю.	14	20
4	Тема 4. Захист оптичних та візуальних каналів витоку інформації. Захист від візуального спостереження та відеозйомки. Лазерні засоби зняття інформації. Методи захисту від оптичного перехоплення. Організація режиму секретності в приміщеннях.	14	20
5	Тема 5. Апаратні засоби контролю доступу та фізичного захисту. Системи контролю та управління доступом (СКУД). Біометричні ідентифікатори. Засоби фізичного блокування та охорони периметру. Інтеграція засобів фізичного захисту в загальну систему безпеки.	14	20
6	Тема 6. Спеціалізовані технічні засоби та комплекси захисту. Огляд сучасних програмно-апаратних комплексів ТЗІ. Генератори шуму та активні засоби захисту. Системи виявлення закладних пристроїв. Вимоги до сертифікації технічних засобів.	14	18
7	Тема 7. Технічний контроль та інспектування захищеності об'єктів. Методики проведення спеціальних перевірок приміщень. Контроль ефективності заходів ТЗІ. Документальне оформлення результатів технічного контролю. Взаємодія з державними експертними органами.	14	20
8	**Всього**	**98**	**138**

7. ВИДИ ТА МЕТОДИ КОНТРОЛЮ

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

1. Дайте визначення поняття «технічний захист інформації» (ТЗІ).
2. Які основні принципи побудови системи ТЗІ?
3. Що таке інформаційна безпека та як вона співвідноситься з ТЗІ?
4. Назвіть основні загрози інформації в технічних каналах витоку.
5. Поясніть різницю між організаційними та технічними заходами захисту.
6. Які нормативні документи регламентують ТЗІ в Україні?
7. Що таке державна експертиза у сфері ТЗІ?
8. Які міжнародні стандарти (ISO/IEC) застосовуються для систем ТЗІ?
9. Які вимоги до акредитації спеціалізованих організацій у сфері ТЗІ?
10. Поясніть роль криптографічного захисту в системі ТЗІ.
11. Які основні методи захисту від електромагнітного випромінювання?
12. Що таке екранування та які його види?
13. Поясніть принцип роботи генераторів шуму для захисту інформації.
14. Які методи контролю каналів побічних електромагнітних випромінювань?
15. Назвіть основні засоби захисту від несанкціонованого доступу до комп’ютерних систем.
16. Як здійснюється аудит системи ТЗІ?
17. Які етапи створення комплексної системи захисту інформації?
18. Опишіть процедуру тестування ефективності технічних засобів захисту.
19. Які методи використовуються для виявлення закладних пристроїв?
20. Як організовується контроль доступу до приміщень з обмеженим доступом?
21. Які новітні технології застосовуються для захисту інформації?
22. Як штучний інтелект використовується у сфері ТЗІ?
23. Які особливості захисту інформації в хмарних технологіях?
24. Поясніть роль систем моніторингу та SIEM у ТЗІ.
25. Які перспективи розвитку стандартів у сфері ТЗІ?
26. Розробіть приклад структури комплексної системи ТЗІ для університету.
27. Які основні відмінності між захистом інформації у державних та комерційних структурах?
28. Як поєднуються організаційні, правові та технічні заходи у системі ТЗІ?
29. Які ризики виникають при недотриманні вимог ТЗІ?
30. Сформулюйте критерії оцінки ефективності системи ТЗІ.

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

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

<u>ЕКЗАМЕН</u>

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 за заданою тематикою	Відповідно до робочої програми та розкладу занять	Розгляд відповідного матеріалу під час аудиторних занять або ІКР[1], 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 та розкладу 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

[1] Індивідуально-консультативна робота викладача зі здобувачами

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 ЕКЗАМЕН
(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.

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

- за підготовку до аудиторних занять (максимум 60 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 12;
- за виконання завдань для самостійного опрацювання (тестування, завдання, підготовка реферату (есе) за заданою тематикою) (максимум 20 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 4;
- за інші види індивідуальних завдань, в т.ч. підготовку наукових публікацій, участь у роботі круглих столів, конференцій тощо (максимум 20- 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 4.

9. КРИТЕРІЇ ЗАГАЛЬНИХ РЕЗУЛЬТАТІВ ОЦІНЮВАННЯ ЗНАНЬ ЗДОБУВАЧІВ

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		

10. 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. НД ТЗІ 3.7-003-05. Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі. – Затверджено наказом ДСТСЗІ СБ України № 125 від 8.11.2005.
5. НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу. – Затверджено наказом ДСТСЗІ СБ України № 22 від 28.04.99.
6. НД ТЗІ 2.5-005-99. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу. – Затверджено наказом ДСТСЗІ СБ України № 22 від 28.04.1999.
7. Положення про Державну експертизу в сфері технічного захисту інформації. – Затверджено наказом Адміністрації ДССЗЗІ України № 93 від 16.05.07.
8. 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.
9. Богуш В.М., Кривуца В.Г., Кудін А.М. Інформаційна безпека: Термінологічний навчальний довідник/ За ред. Кривуци В.Р – Київ.: ООО"Д.В.К.", 2004. – 508 с.

Допоміжна

1. ДСТУ ISO/IEC 27002:2015 Інформаційні технології. Методи захисту. Звід практик щодо заходів інформаційної безпеки.
2. ДСТУ 3396.1-96. Захист інформації. Технічний захист інформації. Порядок проведення робіт.
3. 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.
4. НД ТЗІ 1.4-001-2000. Типове положення про службу захисту інформації в автоматизованій системі.
5. 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.
6. 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.

Інформаційні ресурси

10. Національна бібліотека України ім. В.І. Вернадського : веб-сайт. URL: http://www.nbuv.gov.ua.
11. Он-лайн бібліотека. URL: http://www.lib.com.ua
12. http://www.info-library.com.ua/books-book-149.html
13. https://owasp.org – OWASP
14. Сайт Державної служби спеціального зв'язку та захисту інформації. URL: https://cip.gov.ua/ua
15. Сайт Технічний захист інформації. URL: https://tzi.ua/ua/index.html
16. Комплексні системи захисту інформації. URL: https://web.posibnyky.vntu.edu.ua/fmib/41yaremchuk_kompleksni_systemy_zahystu_informaciyi/
17. 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
18. Сайт Computer Emergency Response Team of Ukraine. URL: https://cert.gov.ua
19. https://zakon.rada.gov.ua/laws