СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ
«ПРОЄКТУВАННЯ СИСТЕМ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ»

<table>
<tr><td colspan="3">Лектор курсу</td><td colspan="2">Пепа Юрій Володимирович,
кандидат технічних наук, доцент,
професор кафедри Технічних систем кіберзахисту</td><td colspan="2">Контактна інформація лектора (e-mail),
сторінка курсу в GWE</td><td colspan="2">e-mail: y.pepa@duikt.edu.ua
сторінка курсу в Classroom:
https://classroom.google.com/c/ODQ1NDY2NTk3NzEz?cjc=2rofmz3j
код доступу – 2rofmz3j</td></tr>
<tr><td colspan="3">Галузь знань</td><td colspan="2">12 Інформаційні технології</td><td colspan="2">Рівень вищої освіти</td><td colspan="2">Магістр</td></tr>
<tr><td colspan="3">Спеціальність</td><td colspan="2">F5 Кібербезпека та захист інформації</td><td colspan="2">Семестр</td><td colspan="2">1</td></tr>
<tr><td colspan="3">Освітня програма</td><td colspan="2">Кібербезпека</td><td colspan="2">Тип дисципліни</td><td colspan="2">Цикл вибіркових компонент ОНП</td></tr>
<tr><td rowspan="2">Обсяг:</td><td>Кредитів ECTS</td><td>Годин</td><td colspan="5">За видами занять:</td></tr>
<tr><td>5</td><td>150</td><td>Лекцій
24</td><td>Семінарських занять
-</td><td>Практичних занять
18</td><td>Лабораторних занять
12</td><td>Самостійна підготовка
96</td></tr>
<tr><td colspan="9">АНОТАЦІЯ КУРСУ</td></tr>
<tr><td colspan="9">Взаємозв’язок у структурно-логічній схемі</td></tr>
<tr><td colspan="3">Освітні компоненти, які передують вивченню</td><td colspan="6">Методи та засоби технічного захисту інформації; комплексні системи захисту інформації; основи кібербезпеки; управління інформаційною безпекою; нормативне забезпечення ТЗІ.</td></tr>
<tr><td colspan="3">Освітні компоненти для яких є базовою</td><td colspan="6">Переддипломна практика; кваліфікаційна робота магістра; аудит та експертиза систем захисту інформації; управління проєктами кіберзахисту.</td></tr>
<tr><td>Мета курсу:</td><td colspan="8">формування здатності магістрів проєктувати системи технічного захисту інформації для об’єктів інформаційної діяльності з урахуванням моделі загроз, категорії інформації, архітектури об’єкта, нормативних вимог, оцінювання ризиків, технічних каналів витоку та процедур впровадження, випробування й супроводу системи ТЗІ.</td></tr>
<tr><td colspan="9">Компетентності відповідно до освітньої програми</td></tr>
<tr><td colspan="4">Soft-skills / Загальні компетентності (КЗ)</td><td colspan="5">Hard-skills / Фахові компетентності (КФ)</td></tr>
<tr><td colspan="4">КЗ1. Здатність застосовувати знання у практичних ситуаціях.
КЗ3. Здатність до абстрактного мислення, аналізу та синтезу.
КЗ4. Здатність оцінювати та забезпечувати якість виконуваних робіт.
КЗ7. Вміння виявляти, ставити та вирішувати проблеми.
КЗ9. Здатність до пошуку, оброблення та аналізу інформації з різних джерел.
КЗ10. Здатність застосовувати кращі практики у професійній діяльності.</td><td colspan="5">КФ2. Здатність розробляти, впроваджувати та аналізувати нормативні документи, положення, інструкції й вимоги технічного та організаційного спрямування, а також інтегрувати, аналізувати і використовувати кращі світові практики, стандарти у професійній діяльності в сфері інформаційної безпеки та/або кібербезпеки.
КФ3. Здатність досліджувати, розробляти і супроводжувати методи та засоби інформаційної безпеки та/або кібербезпеки на об’єктах інформаційної діяльності та критичної інфраструктури.
КФ5. Здатність до дослідження, системного аналізу та забезпечення безперервності бізнес/операційних процесів з метою визначення вразливостей інформаційних систем та ресурсів, аналізу ризиків та визначення оцінки їх впливу у відповідності до встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.
КФ8. Здатність досліджувати, розробляти, впроваджувати та супроводжувати методи і засоби криптографічного та технічного захисту інформації на об’єктах інформаційної діяльності та критичної інфраструктури, в інформаційних системах, а також здатність оцінювати ефективність їх використання, згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.
КФ9. Здатність аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес/операційних процесів в галузі інформаційної безпеки та/або кібербезпеки організації в цілому.
КФ12. Здатність розробляти технічну документацію для проведення тестування, налагоджування та допоміжних заходів щодо функціонування та експлуатації систем захисту інформації на об'єктах інформаційної діяльності.</td></tr>
</table>

Програмні результати навчання (РН)

РН6. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення.
РН7. Обґрунтовувати використання, впроваджувати та аналізувати кращі світові стандарти, практики з метою розв'язання складних задач професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.
РН8. Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.
РН10. Забезпечувати безперервність бізнес/операційних процесів, а також виявляти уразливості інформаційних систем та ресурсів, аналізувати та оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації.
РН13. Досліджувати, розробляти, впроваджувати та використовувати методи та засоби криптографічного та технічного захисту інформації бізнес/операційних процесів, а також аналізувати і надавати оцінку ефективності їх використання в інформаційних системах, на об'єктах інформаційної діяльності та критичної інфраструктури.
РН14. Аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес/операційних процесів у сфері інформаційної та/або кібербезпеки в цілому.
РН15. Зрозуміло і недвозначно доносити власні висновки з проблем інформаційної безпеки та/або кібербезпеки, а також знання та пояснення, що їх обґрунтовують до персоналу, партнерів та інших осіб.
РН16. Приймати обґрунтовані рішення з організаційно-технічних питань інформаційної безпеки та/або кібербезпеки у складних і непередбачуваних умовах, у тому числі із застосуванням сучасних методів та засобів оптимізації, прогнозування та прийняття рішень.
РН19. Обирати, аналізувати і розробляти придатні типові аналітичні, розрахункові та експериментальні методи кіберзахисту, розробляти, реалізовувати та супроводжувати проекти з захисту інформації у кіберпросторі, інноваційної діяльності та захисту інтелектуальної власності.
РН23. Обґрунтовувати вибір програмного забезпечення, устаткування та інструментів, інженерних технологій і процесів, а також обмежень щодо них в галузі інформаційної безпеки та/або кібербезпеки на основі сучасних знань у суміжних галузях, наукової, технічної та довідкової літератури та іншої доступної інформації.

ОРГАНІЗАЦІЯ НАВЧАННЯ

Тема, опис теми	Вид заняття	Оцінювання за тему	Форми і методи навчання/питання до самостійної роботи
Тема 1: «Методологічні основи проєктування систем ТЗІ». **Знати:** поняття системи ТЗІ, життєвий цикл проєктування, етапи створення комплексної системи захисту інформації, склад проєктної документації та нормативну базу. **Вміти:** визначати об'єкт захисту, межі системи, ролі учасників проєкту та вихідні дані для проєктування. **Формування компетентностей:** КЗ1, КЗ3, КЗ9, КЗ10; КФ2, КФ3, КФ12. **Результати навчання:** РН7, РН8, РН23. **Рекомендовані джерела:** 1-10.			
Система ТЗІ як об'єкт проєктування.	Лекція 1 2 год	-	Лекція-презентація, проблемне обговорення, експрес-опитування.
Опис об'єкта інформаційної діяльності: активи, приміщення, інформаційні потоки, зони доступу.	Практичне заняття 1 2 год	4 бали	Практичне завдання, короткий звіт, захист результатів.
Нормативно-методична база проєктування систем ТЗІ.	Лекція 2 2 год	-	Лекція-презентація, проблемне обговорення, експрес-опитування.
Формування вихідних даних і переліку вимог до системи ТЗІ.	Практичне заняття 2 2 год	4 бали	Практичне завдання, короткий звіт, захист результатів.
Життєвий цикл створення системи ТЗІ.	Лекція 3 2 год	-	Лекція-презентація, проблемне обговорення, експрес-опитування.
Побудова структурної схеми об'єкта захисту та визначення меж системи ТЗІ.	Лабораторна робота 1 2 год	2 бали	Лабораторне моделювання, робота зі схемами, вимогами та тестовими даними, оформлення проєктної документації.

Оформлення паспорта об’єкта захисту та початкового переліку активів.	Лабораторна робота 2 2 год	2 бали	Лабораторне моделювання, робота зі схемами, вимогами та тестовими даними, оформлення проєктної документації.
Тема 1: «Вихідні дані для проєктування системи ТЗІ: опис об’єкта, активи, інформаційні потоки, зони безпеки».	Самостійна робота 1 24 год	3 балів	Самостійна підготовка за джерелами, оформлення матеріалів до захисту.
Тема 2: «Модель загроз, технічні канали витоку та оцінювання ризиків». **Знати:** типові загрози для об’єктів інформаційної діяльності, моделі порушника, методи аналізу технічних каналів витоку та підходи до оцінювання ризиків. **Вміти:** формувати модель загроз, визначати актуальні канали витоку та встановлювати пріоритети захисних заходів. **Формування компетентностей:** К31, К33, К37, К39; КФ3, КФ5, КФ8. **Результати навчання:** РН6, РН10, РН13. **Рекомендовані джерела:** 5-18.			
Ідентифікація загроз і модель порушника.	Лекція 4 2 год	-	Лекція-презентація, проблемне обговорення, експрес-опитування.
Розроблення моделі загроз і матриці ризиків для об’єкта ТЗІ.	Практичне заняття 3 2 год	4 бали	Практичне завдання, короткий звіт, захист результатів.
Технічні канали витоку інформації.	Лекція 5 2 год	-	Лекція-презентація, проблемне обговорення, експрес-опитування.
Аналіз акустичних, віброакустичних, електромагнітних та побічних каналів витоку.	Практичне заняття 4 2 год	4 бали	Практичне завдання, короткий звіт, захист результатів.
Оцінювання ризиків і визначення вимог до захисту.	Лекція 6 2 год	-	Лекція-презентація, проблемне обговорення, експрес-опитування.
Побудова матриці актуальності загроз і вибір пріоритетних напрямів захисту.	Лабораторна робота 3 2 год	4 бали	Лабораторне моделювання, робота зі схемами, вимогами та тестовими даними, оформлення проєктної документації.
Тема 2: «Модель загроз і ризиків: порушник, технічні канали витоку, матриця пріоритетності захисних заходів».	Самостійна робота 2 24 год	3 балів	Самостійна підготовка за джерелами, оформлення матеріалів до захисту.
Тема 3: «Проєктні рішення та технічна архітектура системи ТЗІ». **Знати:** принципи побудови архітектури системи ТЗІ, склад організаційних, інженерно-технічних і програмно-технічних заходів, вимоги до документації. **Вміти:** обирати засоби захисту, формувати структурні схеми, специфікації та технічне завдання. **Формування компетентностей:** К31, К33, К34, К37, К310; КФ2, КФ3, КФ8, КФ12. **Результати навчання:** РН7, РН8, РН13, РН16, РН19, РН23. **Рекомендовані джерела:** 5-18.			
Архітектура системи ТЗІ та принципи комплексності захисту.	Лекція 7 2 год	-	Лекція-презентація, проблемне обговорення, експрес-опитування.
Розроблення структурної схеми системи ТЗІ для навчального об’єкта.	Практичне заняття 5 2 год	4 бали	Практичне завдання, короткий звіт, захист результатів.

Організаційні, інженерно-технічні та програмно-технічні заходи захисту.	Лекція 8 2 год	-	Лекція-презентація, проблемне обговорення, експрес-опитування.
Підбір засобів ТЗІ та формування специфікації обладнання/програмних засобів.	Практичне заняття 6 2 год	4 бали	Практичне завдання, короткий звіт, захист результатів.
Технічне завдання і комплект проєктної документації.	Лекція 9 2 год	-	Лекція-презентація, проблемне обговорення, експрес-опитування.
Розроблення фрагмента технічного завдання на систему ТЗІ.	Практичне заняття 7 2 год	4 бали	Практичне завдання, короткий звіт, захист результатів.
Моделювання розміщення засобів контролю доступу, екранування та захисту каналів витоку.	Лабораторна робота 4 2 год	2 год 2 бали	Лабораторне моделювання, робота зі схемами, вимогами та тестовими даними, оформлення проєктної документації
Розроблення плану впровадження системи ТЗІ з календарним графіком та відповідальними особами.	Лабораторна робота 5 2 год	2 год 2 бали	Лабораторне моделювання, робота зі схемами, вимогами та тестовими даними, оформлення проєктної документації
Тема 3: «Фрагмент проєкту системи ТЗІ: структурна схема, специфікація засобів, технічне завдання, план впровадження».	Самостійна робота 3 24 год	3 балів	Самостійна підготовка за джерелами, оформлення матеріалів до захисту.
Тема 4: «Впровадження, випробування, оцінювання ефективності та супровід системи ТЗІ». **Знати:** порядок монтажу, налаштування, випробувань, контролю ефективності, документування та супроводу системи ТЗІ. **Вміти:** планувати приймальні випробування, готувати звітність, аналізувати результати контролю та пропонувати коригувальні заходи. **Формування компетентностей:** КЗ1, КЗ4, КЗ7, КЗ10; КФ3, КФ8, КФ9, КФ12. **Результати навчання:** РН6, РН8, РН13, РН14, РН15, РН16, РН19. **Рекомендовані джерела:** 5-18.			
Впровадження проєктних рішень і контроль виконання робіт.	Лекція 10 2 год	-	Лекція-презентація, проблемне обговорення, експрес-опитування.
Підготовка програми та методики випробувань системи ТЗІ.	Практичне заняття 8 2 год	4 бали	Практичне завдання, короткий звіт, захист результатів.
Контроль ефективності, аудит і супровід системи ТЗІ.	Лекція 11 2 год	-	Лекція-презентація, проблемне обговорення, експрес-опитування.
Комплексна tabletop-вправа із захисту проєктного рішення системи ТЗІ.	Практичне заняття 9 2 год	4 бали	Практичне завдання, короткий звіт, захист результатів.
Оцінювання відповідності та удосконалення системи ТЗІ.	Лекція 12 2 год	-	Лекція-презентація, проблемне обговорення, експрес-опитування.
Захист індивідуального проєкту системи ТЗІ для об’єкта інформаційної діяльності.	Лабораторна робота 6 2 год	2 год 2 бали	Лабораторне моделювання, робота зі схемами, вимогами та тестовими даними, оформлення проєктної документації.
Тема 4: «Індивідуальний проєкт системи ТЗІ: обґрунтування рішень, випробування, ризики впровадження, супровід».	Самостійна робота 3	3 балів	Самостійна підготовка за джерелами, оформлення матеріалів до захисту.

	24 год		

МАТЕРІАЛЬНО-ТЕХНІЧНЕ ЗАБЕЗПЕЧЕННЯ ДИСЦИПЛІНИ

Комп'ютерний клас або персональні комп'ютери здобувачів, мультимедійний проєктор, мережа Інтернет.
Віртуальне навчальне середовище Google Workspace / Google Classroom.
Шаблони опису об’єкта захисту, моделі загроз, технічного завдання, структурної схеми, специфікації засобів ТЗІ, програми та методики випробувань.
Навчальні або демонстраційні засоби проєктування, моделювання та документування: draw.io / diagrams.net, Microsoft Visio, LibreOffice Draw, офісні пакети, тестові приклади об’єктів інформаційної діяльності.
Нормативні документи з кібербезпеки, захисту інформації, технічного захисту інформації та створення КСЗІ.

ІНФОРМАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ ДИСЦИПЛІНИ

1. Закон України «Про захист інформації в інформаційно-комунікаційних системах». https://zakon.rada.gov.ua/
2. Закон України «Про основні засади забезпечення кібербезпеки України». https://zakon.rada.gov.ua/
3. НД ТЗІ 1.1-003-99. Термінологія в галузі захисту інформації в комп’ютерних системах від несанкціонованого доступу.
4. НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу.
5. НД ТЗІ 2.5-005-99. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності.
6. НД ТЗІ 3.7-003-05. Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі.
7. НД ТЗІ 3.6-001-2000. Технічний захист інформації. Комп’ютерні системи. Порядок створення, впровадження, супроводження та модернізації засобів технічного захисту інформації.
8. ДСТУ ISO/IEC 27001:2023. Інформаційна безпека, кібербезпека та захист приватності. Системи керування інформаційною безпекою. Вимоги.
9. ДСТУ ISO/IEC 27002:2023. Заходи керування інформаційною безпекою.
10. ISO/IEC 27005:2022. Information security, cybersecurity and privacy protection — Guidance on managing information security risks.
11. NIST SP 800-30 Rev. 1. Guide for Conducting Risk Assessments. https://csrc.nist.gov/
12. NIST SP 800-53 Rev. 5. Security and Privacy Controls for Information Systems and Organizations. https://csrc.nist.gov/
13. ENISA. Risk Management and Information Security Guidance. https://www.enisa.europa.eu/
14. Держспецзв’язку України. Нормативні документи у сфері технічного захисту інформації. https://cip.gov.ua/
15. Методичні матеріали з розроблення технічного завдання, моделі загроз, програми та методики випробувань систем ТЗІ.

ПОЛІТИКА КУРСУ («ПРАВИЛА ГРИ»)

Курс передбачає роботу в колективі, аналіз реалістичних об’єктів інформаційної діяльності та аргументований захист прийнятих проєктних рішень.
Середовище в аудиторії є відкритим до конструктивної критики, професійної дискусії та коректного обговорення недоліків архітектури захисту.
Освоєння дисципліни передбачає відвідування лекцій, практичних і лабораторних занять, а також системну самостійну роботу.
Усі завдання мають бути виконані у встановлений термін. У разі поважної причини відсутності здобувач погоджує з викладачем порядок відпрацювання.
Під час виконання завдань потрібно посилатися на використані джерела, не розголошувати чутливі дані про об’єкти захисту та дотримуватися правил академічної доброчесності.

КРИТЕРІЇ ТА МЕТОДИ ОЦІНЮВАННЯ

Умовою допуску до підсумкового контролю є набрання здобувачем 60 балів у сукупності за всіма темами дисципліни.

Форми контролю	**Види навчальної роботи**	Оцінювання
ПОТОЧНИЙ КОНТРОЛЬ	• Виконання практичних робіт	36 балів
	• Виконання лабораторних робіт	12 балів
	• Самостійна робота	12 балів
ПІДСУМКОВЕ ОЦІНЮВАННЯ ***Залік***	Метою *заліку* є контроль сформованості практичних навичок та професійних компетентностей.	40 балів

Додаткова оцінка

Види навчальної роботи	Оцінювання
Участь у наукових конференціях, підготовка наукових публікацій за тематикою освітньої компоненти:	
- тези доповіді на фаховій конференції;	2 бали
- стаття у фаховому виданні України;	6 балів
- стаття в іноземному рецензованому виданні.	10 балів
Максимальна кількість додаткових балів, які можуть бути зараховані здобувачу освіти – 10 балів.	

ПІДСУМКОВА ОЦІНКА ЗА ДИСЦИПЛІНУ

БАЛИ	Критерії оцінювання	Рівень компетентності	Оцінка / *запис в заліковій відомості*
90-100	Здобувач демонструє повні й міцні знання навчального матеріалу в обсязі, що відповідає силабусу дисципліни, правильно й обґрунтовано приймає рішення в різних нестандартних ситуаціях проєктування систем ТЗІ. Вміє реалізувати теоретичні положення дисципліни у практичних завданнях: класифікує проєктне рішенняи, визначає рівень ризику, формує порядок ескалації, обирає заходи локалізації, відновлення та післяпроєктне рішенняного вдосконалення системи ТЗІ. Знає сучасні підходи НД ТЗІ, ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27005, принципи створення КСЗІ, вимоги до технічного завдання, моделі загроз, випробувань і звітності. Під час практичних і лабораторних робіт самостійно розв'язує поставлені завдання, активно бере участь у дискусіях, аргументує власну позицію та здатний захищати прийняті рішення.Зменшення 100-бальної оцінки може бути пов'язане з неповним розкриттям окремих питань, які виходять за межі основного обсягу курсу, або з невпевненістю у тлумаченні складних практичних ситуацій.	**Високий** Повністю забезпечує вимоги до знань, умінь і навичок, визначених силабусом дисципліни. Власні пропозиції здобувача щодо оцінювання проєктних рішень, удосконалення процесів проєктування та підвищення ефективності системи ТЗІ демонструють здатність використовувати знання, отримані під час вивчення цієї та суміжних дисциплін.	Відмінно / Зараховано (A)
82-89	Здобувач демонструє гарні знання, добре володіє матеріалом, що відповідає силабусу дисципліни, робить на його основі аналіз можливих ситуацій та вміє застосовувати теоретичні положення під час вирішення практичних задач проєктування систем ТЗІ, але допускає окремі неточності. Вміє самостійно виправляти допущені помилки, кількість яких є незначною. Знає сучасні технології та методи виявлення, тріажу, локалізації, документування й аналізу причин проєктних рішень. Під час виконання практичних і лабораторних завдань дає вичерпні пояснення щодо прийнятих рішень, однак окремі висновки можуть потребувати уточнення або додаткового обґрунтування.	**Достатній** Забезпечує здобувачу самостійне вирішення основних практичних задач в умовах, коли вихідні дані змінюються порівняно з прикладами, що розглядались під час вивчення дисципліни. Здатний адаптувати типові playbook-и та процедури проєктування до конкретного об'єкта ТЗІ.	Добре / Зараховано (B)
75-81	Здобувач загалом добре володіє матеріалом, знає основні положення курсу, робить на їх основі аналіз можливих ситуацій та вміє застосовувати їх під час вирішення типових практичних завдань, але допускає окремі неточності. Вміє пояснити основні етапи виконаних завдань, визначити категорію системи ТЗІ, запропонувати порядок проєктування, підготувати базовий звіт і дати правильні відповіді у разі зміни вихідних параметрів. Помилки у відповідях, рішеннях або висновках не є системними. Знає характеристики основних процесів, що мають визначальне значення для проєктування систем ТЗІ в системах ТЗІ.	**Достатній** Конкретний рівень за вивченим матеріалом силабусу дисципліни. Додаткові питання щодо використання теоретичних положень у нестандартних практичних ситуаціях можуть викликати утруднення, однак основні задачі курсу виконуються.	Добре / Зараховано (C)

67-74	Здобувач засвоїв основний теоретичний матеріал, передбачений силабусом дисципліни, та розуміє постановку стандартних практичних завдань. Має пропозиції щодо напрямів їх вирішення, розуміє основні положення, що є визначальними в курсі, може виконувати подібні завдання до тих, що розглядалися з викладачем.Під час аналізу проєктних рішень, заповнення шаблонів звітності, побудови матриці ризиків або опису процедури ескалації допускає значну кількість неточностей і грубих помилок, які може усувати за допомогою викладача. .	**Середній** Забезпечує достатньо надійний рівень відтворення основних положень дисципліни. Здобувач здатний виконувати типові завдання за наданим алгоритмом, але потребує підтримки під час аналізу складних або неповних вихідних даних.	Задовільно / Зараховано (D)
60-66	Здобувач має певні знання, передбачені силабусом дисципліни, володіє основними положеннями на рівні, який визначається як мінімально допустимий. З використанням базових теоретичних положень з труднощами пояснює правила вирішення практичних, лабораторних або розрахунково-аналітичних завдань. Виконання практичних, лабораторних та індивідуальних завдань значною мірою формалізоване: є відповідність запропонованому алгоритму, але відсутнє глибоке розуміння взаємозв'язків між виявленням, тріажем, локалізацією, відновленням, документуванням і післяпроєктне рішенняним аналізом.	**Середній** Є мінімально допустимим у всіх складових навчальної програми з дисципліни. Здобувач може відтворити базовий порядок дій під час проєктування, але не демонструє достатньої самостійності в обґрунтуванні рішень.	Задовільно / Зараховано (E)
35-59	Здобувач може відтворити окремі фрагменти з курсу. Незважаючи на те, що окремі завдання навчальної дисципліни виконувались, працював пасивно, відповіді під час практичних і лабораторних робіт у більшості випадків є неповними, невірними або необґрунтованими. Цілісність розуміння матеріалу з дисципліни відсутня. Здобувач не може самостійно визначити рівень ризику системи ТЗІ, послідовність проєктування, вимоги до доказів, структуру проєктної документації або заходи післяпроєктне рішенняного вдосконалення системи ТЗІ.	**Низький** Не забезпечує практичної реалізації задач, що формуються під час вивчення дисципліни. Знання мають фрагментарний характер і не дозволяють виконувати професійні завдання без повторного опрацювання матеріалу.	Незадовільно з можливістю повторного складання) / Не зараховано (FX) *В залікову книжку не проставляється*
0-34	Здобувач повністю не виконав вимог силабусу навчальної дисципліни. Його знання на підсумкових етапах навчання є фрагментарними або відсутніми. Практичні, лабораторні та самостійні завдання не виконані або виконані на рівні, що не дозволяє оцінити сформованість результатів навчання. Здобувач не допущений до складання заліку або не може продемонструвати мінімально необхідні знання щодо проєктування систем ТЗІ в системах ТЗІ.	**Незадовільний** Здобувач не підготовлений до самостійного вирішення задач, які окреслює мета та завдання дисципліни. Потребує повторного вивчення навчального матеріалу.	Незадовільно з обов’язковим повторним вивченням / Не допущений (F) *В залікову книжку не проставляється*

ПОЛІТИКА ДОБРОЧЕСНОСТІ

Здобувач вищої освіти виконуючи самостійну або індивідуальну роботу повинен дотримуватись політики доброчесності.

У разі наявності плагіату в будь-яких видах робіт здобувача, він отримує незадовільну оцінку і повинен повторно виконати завдання, які передбачені у Силабусі.