Затверджено
завідувач кафедри
СТКБ_____ Г. Гайдур

«31» 08 2026 р.

СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ
"Технології розробки і тестування програмного забезпечення систем ІКБ"

Лектор курсу	**Зибін Сергій Вікторович,** доктор технічних наук, професор, професор кафедри систем та технологій кібербезпеки	**Контактна інформація лектора (e-mail), сторінка курсу в GWE**	**e-mail:** s.zybin@duikt.edu.ua **сторінка курсу в Classroom -** https://classroom.google.com/c/NzA4MzAxMjcxNDE5?cjc=nkprc4p **код доступу** - ut62666	
Галузь знань	F Інформаційні технології	**Рівень вищої освіти**	магістр	
Спеціальність	F5 Кібербезпека та захист інформації	**Семестр**	2	
Освітня програма	Кібербезпека та захист інформації	**Тип дисципліни**	Вибіркова компонента освітньо-професійної програми	

Обсяг:	Кредитів ECTS	Годин	За видами занять:				
			Лекцій	Семінарських занять	Практичних занять	Лабораторних занять	Самостійна підготовка
	5	150	18	–	18	18	96

АНОТАЦІЯ КУРСУ

Взаємозв'язок у структурно-логічній схемі

Освітні компоненти, які передують вивченню	Дисципліни професійної підготовки
Освітні компоненти для яких є базовою	Кваліфікаційна робота

Мета курсу: Формування сукупності знань та вмінь щодо застосування методів та засобів розробки і тестування програмного забезпечення систем ІКБ, а також засобів ручного тестування ПЗ, особливостей системного, модульного та інтеграційного тестування, моделей оцінки ступеню тестування програмного продукту, використовувати методи ручного та автоматизованого тестування.

Компетентності відповідно до освітньої програми

Soft- skills / Загальні компетентності (ЗК)	**Hard-skills / Спеціальні компетентності (СК)**
КЗ1. Здатність застосовувати знання у практичних ситуаціях. КЗ2. Здатність до абстрактного мислення, аналізу та синтезу. КЗ4. Здатність оцінювати та забезпечувати якість виконуваних робіт КЗ6. Знання та розуміння предметної області і професійної діяльності. КЗ8. Здатність використовувати інформаційні та комунікаційні технології. КЗ9. Здатність до пошуку, оброблення та аналізу інформації з різних джерел. КЗ10. Здатність застосовувати кращі практики у професійній діяльності.	КФ1. Здатність обґрунтовано застосовувати, інтегрувати, розробляти та удосконалювати сучасні інформаційні технології, фізичні та математичні моделі, а також технології створення та використання прикладного і спеціалізованого програмного забезпечення для вирішення професійних задач у сфері інформаційної безпеки та/або кібербезпеки. 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. 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.

Програмні результати навчання (ПРН)

РН2. Інтегрувати фундаментальні та спеціальні знання для розв'язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах.
РН5. Критично осмислювати проблеми інформаційної безпеки та/або кібербезпеки, у тому числі на міжгалузевому та міждисциплінарному рівні, зокрема на основі розуміння нових результатів інженерних і фізико-математичних наук, а також розвитку технологій створення та використання спеціалізованого програмного забезпечення.
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 методи 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.
РН11. Аналізувати, контролювати та забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки та/або кібербезпеки організації.
РН20. Ставити та вирішувати складні інженерно-прикладні та наукові задачі інформаційної безпеки та/або кібербезпеки з урахуванням вимог вітчизняних та світових стандартів та кращих практик.
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: Захищений життєвий цикл розробки програмного забезпечення. **Знати**: Основні поняття, визначення та концепції інформаційної та кібербезпеки. Етапи захищеного життєвого циклу розробки ПЗ. Поняття "шкідливе програмне забезпечення". Зміст статичного та динамічного аналізу шкідливих програм. Інструменти та шаблони виявлення, що використовуються при аналізі шкідливих програм. **Вміти**: Вміти застосовувати навички побудови та тестування ПЗ з використанням етапів захищеного життєвого циклу розробки ПЗ. Аналізувати прояви та ознаки шкідливого ПЗ. Визначати види шкідливого ПЗ. Проводити пошук шкідливого ПЗ. Застосовувати методи виявлення ШПЗ. **Формування компетентностей:** К31, К34, К36, К38, К310, КФ1, КФ2, КФ5, КФ9. **Результати навчання:** РН-2, РН-5, РН-6, РН-7, РН-10, РН-11, РН-20, РН-23. **Рекомендовані джерела:** 1-9.			
Основні поняття, визначення та концепції інформаційної та кібербезпеки.	Лекція 1 2 год		Лекція-візуалізація
Виявлення та видалення зловмисних програм.	Практичне заняття 1	4 бали	Оволодіти навичками виявлення та видалення зловмисних програм за допомогою сучасних інструментів. Ознайомитися з

	4 год		процесами ідентифікації, аналізу та очищення системи від шкідливого ПЗ.
Захищений життєвий цикл розробки програмного забезпечення (частина 1).	Лекція 2 2 год		Лекція-візуалізація, експрес-опитування здобувачів.
Аналіз шкідливого програмного забезпечення.	Практичне заняття 2 4 год	4 бали	Оволодіти навичками статичного аналізу зловмисних програм за допомогою сучасних інструментів. Ознайомитися з процесами ідентифікації, аналізу та очищення системи від шкідливого ПЗ.
Захищений життєвий цикл розробки програмного забезпечення. (частина 2).	Лекція 3 2 год		Лекція-візуалізація, експрес-опитування здобувачів.
Підхід DevSecOps.	Практичне заняття 3 4 год	4 бали	Оволодіти навичками застосування підходу DevSecOps, який інтегрує практики безпеки в процес DevOps від початку до розробки, розгортання та експлуатації.
Тема 1: Захищений життєвий цикл розробки програмного забезпечення.	Самостійна робота 1 12 год	8 балів	Самостійна підготовка. Удосконалення отриманих знань та умінь, отриманих (надбаних) за попередніми лекціями та практичними заняттями. Отримати навички виявлення ознак різновидів ШПЗ та застосування підходу DevSecOps.
Тема 2: Виявлення загроз програмному інтерфейсу (API). **Знати:** Концепції кібербезпеки та кіберзлочинності. Основні компоненти та можливості системи управління API. **Вміти**: Аналізувати прояви і ознаки розвідки та атак на інформаційні об'єкти. Вміти виявляти ймовірні вразливості програмному інтерфейсу (API), запобігати застосуванню ШПЗ. **Формування компетентностей:** К31, К36, К310, КФ2, КФ9. **Результати навчання:** РН-2, РН-6, РН-10, РН-20. **Рекомендовані джерела:** 1-9.			
Хакери	Лекція 4 2 год		Лекція-візуалізація, експрес-опитування здобувачів.
Концепції кібербезпеки та кіберзлочинності.	Практичне заняття 4 4 год	4 бали	Ознайомитися з відмінностями між концепціями кібербезпеки та кіберзлочинності, класифікацією хакерів, їх мотивів і рушійної сили.
Безпека API.	Лекція 5 2 год		Лекція-візуалізація, експрес-опитування здобувачів.
Основні компоненти та можливості системи управління API.	Практичне заняття 5 4 год	4 бали	Ознайомитися з основними компонентами та можливостями системи управління API.
Виявлення загроз у безпеці API.	Лекція 6 2 год		Лекція-візуалізація, експрес-опитування здобувачів.
Загрози у безпеці API.	Практичне заняття 6 4 год	4 бали	Дослідження загроз безпеці API (Application Programming Interface).
Тема 2: Виявлення загроз програмному інтерфейсу (API).	Самостійна робота 2 12 год	8 балів	Самостійна підготовка. Удосконалення отриманих знань та умінь, отриманих (надбаних) за попередніми лекціями та практичними заняттями. Отримати навички застосування методів боротьби з ШПЗ.

Тема 3: Вектори атак.
Знати: Типи атак в соціальних мережах. Методи соціальної інженерії. Руткіти: механізми проникнення, маскування руткітів на ПК та методи захисту від них.
Вміти: Аналізувати прояви та ознаки шкідливого ПЗ. Протидіяти атакам в соціальних мережах. Виявляти руткіти та здійснювати заходи протидії руткітам.
Формування компетентностей: К34, К38, КФ1, КФ5.
Результати навчання: РН-5, РН-7, РН-11, РН-23.
Рекомендовані джерела: 1-9.

Вектори атак. Класифікація.	Лекція 7 2 год		Лекція-візуалізація, експрес-опитування здобувачів.
Класифікація атак. Дерево атаки.	Практичне заняття 7 4 год	4 бали	Навчитися використовувати модель OSI для класифікація атак відповідно рівням моделі.
Вектори атак. Зброя ПЗ.	Лекція 8 2 год		Лекція-візуалізація, експрес-опитування здобувачів.
Програмне забезпечення як зброя.	Практичне заняття 8 4 год	4 бали	Отримати навички аналізу шкідливого програмного забезпечення.
Вектори атак. Соціальна інженерія.	Лекція 9 2 год		Лекція-візуалізація, експрес-опитування здобувачів.
Соціальна інженерія, використання, атаки.	Практичне заняття 9 4 год	4 бали	Отримати навички досягнення кіберстійкості шляхом моделювання загроз з Threat Modelling. **Залік.**
Тема 3: Вектори атак. Класифікація. Зброя ПЗ. Соціальна інженерія.	Самостійна робота 2 12 год	8 балів	Самостійна підготовка. Удосконалення отриманих знань та умінь, отриманих (надбаних) за попередніми лекціями та практичними заняттями. Отримати навички виявлення вразливостей, протидії атакам в соціальних мережах, руткітам та ШПЗ.

МАТЕРІАЛЬНО-ТЕХНІЧНЕ ЗАБЕЗПЕЧЕННЯ ДИСЦИПЛІНИ

Комп’ютерне обладнання, мережа Інтернет. Віртуальне навчальне середовище.

ІНФОРМАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ ДИСЦИПЛІНИ

1. Loren Kohnfelder. Designing Secure Software: A Guide for Developers. No Starch Press. 2021. 312 p.
2. Козачок В.А., Гайдур Г.І., Гахов С.О., Хмелевський Р.М., Чумак Н.С. Політики безпеки. Навчальний посібник для студентів вищих навчальних закладів – Київ: ДУТ ННІЗІ, 2020. – 167 с. https://duikt.edu.ua/uploads/l_2225_57006111.pdf
3. Технології захисту інформації в інформаційно-телекомунікаційних системах : навч. посіб. / А. В. Жилін, О. М. Шаповал, О. А. Успенський ; ІСЗЗІ КПІ ім. Ігоря Сікорського. – Київ : КПІ ім. Ігоря Сікорського, Вид-во "Політехніка", 2021. – 213 с. https://ela.kpi.ua/server/api/core/bitstreams/d99a0045-e907-4d17-afc1-5431f67d2444/content
4. Комплексна безпека інформаційних мережевих систем: навчальний посібник для студентів спеціальності 174 "Автоматизація, комп’ютерноінтегровані технології та робототехніка" / Укладачі: А.Г. Микитишин,М.М. Митник, О.С. Голотенко, В.В. Карташов. – Тернопіль : ФОП Паляниця В.А., 2023. – 324 с. https://elartu.tntu.edu.ua/handle/123456789/889
5. Сучасні інформаційні технології в кібербезпеці : монографія / А. С. Довбиш, В. К. Ободяк, І. В. Шелехов та ін. ; за ред. В. К. Ободяка, І. В. Шелехова. – Суми : Сумський державний університет, 2021. – 348 с. https://essuir.sumdu.edu.ua/bitstream-download/123456789/82619/3/Obodiak_kiberbezpeka.pdf
6. Anasuri, S. (2024). Secure Software Development Life Cycle (SSDLC) for AI-Based Applications. *International Journal of Artificial Intelligence, Data Science, and Machine Learning*, *5*(1), 104-116. https://doi.org/10.63282/3050-9262.IJAIDSML-V5I1P110

7. Sharma, I., Kaur, A., Kaushik, K., & Chhabra, G. (2023, July). Machine Learning-Based Detection of API Security Attacks. In International Conference on Data Science and Applications. pp. 285-297. Singapore: Springer Nature Singapore.
8. Jason Ricol. “AI for Secure Software Development: Identifying and Fixing Vulnerabilities with Machine Learning.” December 2022.
9. Tim Abdiukov. Secure by design principles in Agile SDLC: Leveraging Formal Verification and AI Enhanced Code Review in CI/CD Environments. *World Journal of Advanced Engineering Technology and Sciences*, 2023, 09(01): 494–503.
10. Singh, J., & Singh, J. (2022). Assessment of supervised machine learning algorithms using dynamic API calls for malware detection. *International Journal of Computers and Applications*, 44(3), 270-277.

ПОЛІТИКА КУРСУ ("ПРАВИЛА ГРИ")

- Курс передбачає роботу в колективі.
- Середовище в аудиторії є дружнім, творчим, відкритим до конструктивної критики.
- Освоєння дисципліни передбачає обов’язкове відвідування лекцій і семінарських занять, а також самостійну роботу.
- Самостійна робота включає в себе теоретичне вивчення питань, що стосуються тем лекційних занять, які не ввійшли в теоретичний курс, або ж були розглянуті коротко, їх поглиблена проробка за рекомендованою літературою.
- Усі завдання, передбачені програмою, мають бути виконані у встановлений термін.
- Якщо здобувач відсутній з поважної причини, він презентує виконані завдання під час самостійної підготовки та консультації викладача.
- Під час роботи над завданнями не допустимо порушення академічної доброчесності: при використанні Інтернет ресурсів та інших джерел інформації здобувач повинен вказати джерело, використане в ході виконання завдання.

КРИТЕРІЇ ТА МЕТОДИ ОЦІНЮВАННЯ

Умовою допуску до підсумкового контролю є набрання здобувачем 30 балів у сукупності за всіма темами дисципліни.

Форми контролю	**Види навчальної роботи**	Оцінювання
ПОТОЧНИЙ КОНТРОЛЬ	• Виконання практичних робіт	36 балів
	• Самостійна робота	24 бали
ПІДСУМКОВЕ ОЦІНЮВАННЯ ***Залік***	Метою заліку є контроль сформованості практичних навичок та професійних компетентностей, необхідних для виконання професійних обов’язків. Залік: оцінюється завчасно виконане Ессе.	40 балів

Додаткова оцінка

Види навчальної роботи	**Оцінювання**
Участь у наукових конференціях, підготовка наукових публікацій за тематикою освітньої компоненти:	
• Тези доповіді на фаховій конференції.	3 бали
• Стаття у фаховому виданні.	5 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 робочій програмі дисципліни, правильно й обґрунтовано приймає необхідні рішення в різних нестандартних ситуаціях. Вміє реалізувати теоретичні положення дисципліни в практичних розрахунках, аналізувати та співставляти дані об’єктів діяльності фахівця на основі набутих з даної та суміжних дисциплін знань та умінь.	**Високий** Повністю забезпечує вимоги до знань, умінь і навичок, що викладені в робочій програмі дисципліни. Власні пропозиції здобувача в оцінках і вирішенні практичних задач підвищує його вміння	Відмінно / Зараховано (А)

	Знає сучасні технології та методи розрахунків з даної дисципліни. За час навчання при проведенні практичних занять, при виконанні індивідуальних/контрольних завдань проявив вміння самостійно вирішувати поставлені завдання, активно включатись в дискусії, може відстоювати власну позицію в питаннях та рішеннях, що розглядаються. Зменшення 100-бальної оцінки може бути пов'язане з недостатнім розкриттям питань, що стосується дисципліни, яка вивчається, але виходить за рамки об'єму матеріалу, передбаченого робочою програмою, або Здобувач проявляє невпевненість в тлумаченні теоретичних положень чи складних практичних завдань.	використовувати знання, які він отримав при вивчені інших дисциплін, а також знання, набуті при самостійному поглибленому вивчені питань, що відносяться до дисципліни, яка вивчається.	
82-89	Здобувач демонструє гарні знання, добре володіє матеріалом, що відповідає робочій програмі дисципліни, робить на їх основі аналіз можливих ситуацій та вміє застосовувати теоретичні положення при вирішенні практичних задач, але допускає окремі неточності. Вміє самостійно виправляти допущені помилки, кількість яких є незначною. Знає сучасні технології та методи розрахунків з даної дисципліни. За час навчання при проведенні практичних занять, при виконанні індивідуальних / контрольних завдань та поясненні прийнятих рішень, дає вичерпні пояснення.	**Достатній** Забезпечує здобувачу самостійне вирішення основних практичних задач в умовах, коли вихідні дані в них змінюються порівняно з прикладами, що розглянуті при вивчені дисципліни.	Добре / Зараховано (B)
75-81	Здобувач в загальному добре володіє матеріалом, знає основні положення матеріалу, що відповідає робочій програмі дисципліни, робить на їх основі аналіз можливих ситуацій та вміє застосовувати при вирішенні типових практичних завдань, але допускає окремі неточності. Вміє пояснити основні положення виконаних завдань та дати правильні відповіді при зміні результату при заданій зміні вихідних параметрів. Помилки у відповідях/ рішеннях/ розрахунках не є системними. Знає характеристики основних положень, що мають визначальне значення при проведенні практичних занять, при виконанні індивідуальних / контрольних завдань та поясненні прийнятих рішень, в межах дисципліни, що вивчається.	**Достатній** Конкретний рівень, за вивченим матеріалом робочої програми дисципліни. Додаткові питання про можливість використання теоретичних положень для практичного використання викликають утруднення.	Добре / Зараховано (C)
67-74	Здобувач засвоїв основний теоретичний матеріал, передбачений робочою програмою дисципліни, та розуміє постанову стандартних практичних завдань, має пропозиції щодо напрямку їх вирішень. Розуміє основні положення, що є визначальними в курсі, може вирішувати подібні завдання тим, що розглядались з викладачем, але допускає значну кількість неточностей і грубих помилок, які може усувати за допомогою викладача.	**Середній** Забезпечує достатньо надійний рівень відтворення основних положень дисципліни.	Задовільно / Зараховано (D)
60-66	Здобувач має певні знання, передбачені в робочій програмі дисципліни, володіє основними положеннями, що вивчаються на рівні, який визначається як мінімально допустимий. З використанням основних теоретичних положень, здобувач з труднощами пояснює правила вирішення практичних/розрахункових завдань дисципліни. Виконання практичних / індивідуальних / контрольних завдань значно формалізовано: є відповідність алгоритму, але відсутнє глибоке розуміння роботи та взаємозв'язків з іншими дисциплінами.	**Середній** Є мінімально допустимим у всіх складових навчальної програми з дисципліни.	Задовільно / Зараховано (E)
35-59	Здобувач може відтворити окремі фрагменти з курсу. Незважаючи на те, що програму навчальної дисципліни здобувач виконав, працював він пасивно, його відповіді під час практичних робіт в більшості є невірними, необґрунтованими.	**Низький** Не забезпечує практичної реалізації задач, що формуються при вивчені	Незадовільно з можливістю повторного складання) /

	Цілісність розуміння матеріалу з дисципліни у здобувача відсутні.	дисципліни.	Не зараховано (FX) *В залікову книжку не проставляється*
0-34	Здобувач повністю не виконав вимог робочої програми навчальної дисципліни. Його знання на підсумкових етапах навчання є фрагментарними. Здобувач не допущений до здачі екзамену/заліку.	**Незадовільний** Здобувач не підготовлений до самостійного вирішення задач, які окреслює мета та завдання дисципліни.	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.