ДЕРЖАВНИЙ ТОРГОВЕЛЬНО-ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ
СИСТЕМА УПРАВЛІННЯ ЯКІСТЮ
Система забезпечення якості освітньої діяльності та якості вищої освіти
сертифікована на відповідність ДСТУ ISO 9001:2015 / ISO 9001:2015
Кафедра інженерії програмного забезпечення та кібербезпеки

ТЕХНОЛОГІЇ БЕЗПЕКИ ПРОГРАМНИХ ПРОДУКТІВ/
SECURITY TECHNOLOGIES OF SOFTWARE PRODUCTS

СИЛАБУС/
SILABUS

ЗАТВЕРДЖЕНО
засіданням кафедри
(протокол №. 1
від «01» серпня 2024 р.)
завідувач кафедри
_____Олена КРИВОРУЧКО

Київ 2024

Назва освітньої компоненти	**ТЕХНОЛОГІЇ БЕЗПЕКИ ПРОГРАМНИХ ПРОДУКТІВ /** SECURITY TECHNOLOGIES OF SOFTWARE PRODUCTS
Спеціальність	121 «Інженерія програмного забезпечення»
Освітній ступінь	Другий (магістерський)
Освітньо-професійна програма	**УПРАВЛІННЯ ПРОЄКТАМИ ПРОГРАМНИХ ПРОДУКТІВ**
	Лектор: **ЛахноВалерій** -професор кафедри інженерії програмного забезпечення та кібербезпеки на 0,5 ставки -професор кафедри комп'ютерних систем, мереж та кібербезпеки НУБіП -доктор технічних наук -пофесор Резюме викладача: http://surl.li/uyfohc е-пошта: lva964@nubip.edu.ua
	Асистент лектора: **Шестак Ярослав** -директор ІОЦ-ГЦІТ ДТЕУ -старший викладач Резюме викладача: https://knute.edu.ua/blog/read/?pid=43517&uk Науковий профіль: https://knute.edu.ua/blog/read/?pid=46733 е-пошта: shestack@knute.edu.ua
Консультації	https://knute.edu.ua/blog/read/?pid=47103&uk
Програма освітньої компоненти	https://knute.edu.ua/blog/read/?pid=48215
	ЗМІСТ ОСВІТНЬОЇ КОМПОНЕНТИ
Тема 1. Основні принципи безпеки програмних продуктів.	Вступ. Мета та завдання дисципліни. Огляд загальних принципів безпеки (визначення основних термінів та понять у галузі безпеки програмного забезпечення). Загрози та атаки на програмне забезпечення. Класифікація загроз та атак, які можуть бути спрямовані на програми; аналіз ризиків із зазначенням потенційних наслідків.
Тема 2. Системний аналіз безпеки програмного	Системний аналіз безпеки програмного забезпечення. Інтеграція безпеки в архітектуру програмних систем. Використання сучасних платформ для забезпечення безпеки.

забезпечення.	Вплив апаратного забезпечення на безпеку програмного забезпечення.
Тема 3. Архітектура безпеки програмного забезпечення.	Архітектура безпеки програмного забезпечення. Розробка та оцінка безпечних архітектурних рішень. Моделювання загроз у архітектурі програмного забезпечення. Стратегії безпечного дизайну програмних систем. Оцінка ефективності архітектурних рішень у розрізі безпеки.
Тема 4. Організаційні аспекти безпеки програмного забезпечення.	Організаційні аспекти безпеки програмного забезпечення. Управлінські рішення у сфері безпеки інформації. Порівняння альтернатив для безпеки на рівні організації. Оцінка ризиків та управління ними в умовах невизначеності. Впровадження політик та стандартів безпеки.
Тема 5. Методи тестування безпеки програмного забезпечення.	Методи тестування безпеки програмного забезпечення. Розробка тестових сценаріїв для перевірки безпеки. Автоматизоване тестування на наявність вразливостей у ПЗ. Використання інструментів для аналізу безпеки. Тестування захисту від атак в реальному середовищі.
Тема 6. Верифікація та валідація безпеки програмного забезпечення.	Верифікація та валідація безпеки програмного забезпечення. Методи верифікації безпеки. Валідація функціональних вимог з точки зору безпеки. Валідація відповідності стандартам безпеки. Інструменти для підтримки верифікації та валідації.
Тема 7. Управління безпекою в життєвому циклі програмного продукту.	Управління безпекою в життєвому циклі програмного продукту. Вибір технологій для управління безпекою. Автоматизація процесів управління безпекою. Інтеграція безпеки у життєвий цикл розробки ПЗ. Управління змінами в контексті безпеки.
Тема 8. Аудит безпеки програмного забезпечення.	Аудит безпеки програмного забезпечення. Методи проведення аудиту безпеки. Оцінка ефективності існуючих заходів безпеки. Розробка рекомендацій на основі результатів аудиту. Документування та звітування про результати аудиту.
Тема 9. Інтеграція безпеки в DevOps і CI/CD.	Безпека в процесах Continuous Integration/Continuous Deployment (CI/CD). Інтеграція безпеки в DevOps і CI/CD. Впровадження автоматизованих тестів безпеки в CI/CD. Інструменти для інтеграції безпеки в CI/CD. Оцінка ефективності автоматизованих тестів. Управління конфігурацією та секретами. Безпечне зберігання та управління конфіденційною інформацією. Інструменти для автоматизації управління конфігураціями. Інтеграція безпеки в мікросервісну

	архітектуру. Виклики безпеки в контейнеризованих середовищах. Контейнерна безпека та управління вразливостями.
Тема 10. Безпека в багатокористувацьких системах та блокчейн-технології.	Безпека в багатокористувацьких системах та блокчейн-технології. Протоколи консенсусу та їх вплив на безпеку. Механізми консенсусу в блокчейн-системах. Уразливості і атаки на протоколи консенсусу. Оцінка безпеки різних алгоритмів консенсусу. Механізми захисту даних у блокчейн-системах. Захист приватності в блокчейні. Анонімність та конфіденційність транзакцій. Управління ідентифікацією та доступом у блокчейні. Атаки на блокчейн та захист від них. Типи атак на блокчейн-системи. Розробка стратегій захисту від атак.
Тема 11. Політики та технології для забезпечення конфіденційності в програмному забезпеченні.	Політики та технології для забезпечення конфіденційності в програмному забезпеченні. Вбудовані технології конфіденційності. Методи вбудованого захисту даних. Оцінка впливу на продуктивність систем. Виявлення типових помилок і способи їх уникнення.
Тема 12. Динамічне управління безпекою в умовах змінюваних загроз.	Динамічне управління безпекою в умовах змінюваних загроз. Прогнозування і моделювання загроз. Використання статистичних та машинних методів для моделювання загроз. Інструменти для динамічного моніторингу загроз. Адаптивні стратегії безпеки. Інтеграція автоматичних реакцій на нові загрози. Використання ML для виявлення нових загроз.

СПИСОК ОСНОВНИХ РЕКОМЕНДОВАНИХ ДЖЕРЕЛ

1. Бурячок В.Л. Технології забезпечення безпеки мережевої інфраструктури. [Підручник] / В.Л.Бурячок, А.О.Аносов, В.В.Семко, В.Ю.Со-колов, П.М.Складанний. –К.:КУБГ, 2019. – 218с.

2. Anoop Singhal, Theodore Winograd, Karen Scarfone. Guide to secure web services. National Institute of Standards and Technology Special Publication 800-95, 2017. - 128 Pages

3. Elie Saad, Rick Mitchell. Owasp Testing Guide v4. Open Web Application Security Project, 2020. - 453 Pages

4. Andrew Homan. Web Application Security Exploitation and Countermeasures for Modern Web Applications. United States of America, 2020. – 331 *Pages.* ISBN: 978-1-492-08796-0

5. Justin Clarke. SQL Injection Attacks and Defense. Syngress Publishing, Inc., Elsevier, Inc., 2019 - 494 Pages. ISBN 13: 978-1-59749-424-3

РЕЗУЛЬТАТИ ВИВЧЕННЯ ОСВІТНЬОЇ КОМПОНЕНТИ	
Дисципліна забезпечує оволодіння здобувачами вищої освіти загальними та фаховими компетентностями і досягнення ними програмних результатів навчання:	
ЗК01	Здатність до абстрактного мислення, аналізу та синтезу
ЗК02	Здатність спілкуватися іноземною мовою як усно, так і письмово.
ЗК03	Здатність проводити дослідження на відповідному рівні.
СК04	Здатність розвивати і реалізовувати нові конкурентоспроможні ідеї в інженерії програмного забезпечення.
СК07	Здатність критично осмислювати проблеми у галузі інформаційних технологій та на межі галузей знань, інтегрувати відповідні знання та розв'язувати складні задачі у широких або мультидисциплінарних контекстах
СК10	Здатність використовувати підходи до управління проєктами програмних продуктів та їх захисту, які застосовуватимуться протягом проєкту.
РН07	Аналізувати, оцінювати і застосовувати на системному рівні сучасні програмні та апаратні платформи для розв'язання складних задач інженерії програмного забезпечення
РН12	Приймати ефективні організаційно-управлінські рішення в умовах невизначеності та зміни вимог, порівнювати альтернативи, оцінювати ризики
РН16	Планувати, організовувати та здійснювати тестування, верифікацію та валідацію програмного забезпечення.
РН19	*Вміти вибирати й автоматизовано налаштовувати технологію управління програмними продуктами згідно з життєвим циклом програмного продукту та їх захист.*

ОЦІНЮВАННЯ ЗНАНЬ ЗДОБУВАЧІВ ОСВІТИ

Сума балів, накопичених здобувачем вищої освіти за виконання всіх видів поточних навчальних завдань (робіт) на лабораторних/практичних заняттях, свідчить про ступінь оволодіння ним програмою освітньої компоненти на конкретному етапі її вивчення. Протягом семестру здобувачі освіти можуть набрати від 0 до 100 балів, що переводяться у національну шкалу оцінювання і відповідно у шкалу ЄКТС. Кількість балів відповідає певному рівню засвоєння дисципліни

Довідник з розподілу оцінок ДТЕУ (Шкала ЄКТС):

Бали ДТЕУ	Відсоток балів відносно загальної кількості одержаних прохідних балів	Кумулятивний відсоток отриманих прохідних балів
90-100	20	20
82-89	10	зо
75-81	20	50
69-74	10	60
60-68	40	100

Роподіл балів за видами робіт:

Вид роботи	**Бали**	**Вид роботи**	**Бали**
Лабораторна робота 1	3	Самостійна робота 1	2
Лабораторна робота 2	3	Самостійна робота 2	2
Лабораторна робота 3	3	Самостійна робота 3	2
Лабораторна робота 4	3	Самостійна робота 4	2
Лабораторна робота 5	3	Самостійна робота 5	2
Лабораторна робота 6	3	Самостійна робота 6	2
Лабораторна робота 7	3	Самостійна робота 7	2
Лабораторна робота 8	3	Самостійна робота 8	2
Лабораторна робота 9	3	Самостійна робота 9	2
Лабораторна робота 10	3	Самостійна робота 10	2
Лабораторна робота 11	3	Самостійна робота 11	2
Лабораторна робота 12	3	Самостійна робота 12	2
Лабораторна робота 13	3	Самостійна робота 13	2
Лабораторна робота 14	3	Самостійна робота 14	2
Лабораторна робота 15	3	Самостійна робота 15	2
Захист проєкту	15	Наукова робота	10

Вимоги до критеріїв оцінювання самостійної роботи студента (оцінювання одного завдання у відсотковому еквіваленті)	
40%	Детальний розгляд сутності та вмісту основних джерел. Подання фактів, ідей і результатів досліджень у логічній послідовності. Правильно проаналізовано поточний стан дослідження проблеми та зроблено огляд перспектив подальшого розвитку даного питання.
40%	Обґрунтованість аргументів, підтвердження особистого ставлення, пропозиції стосовно вирішення завдання, встановлення напрямків аналізу.
20%	Оформлення звіту у відповідності вимог
Критерії оцінювання самостійної роботи студента (оцінювання одного завдання у відсотковому еквіваленті)	
100%	В повному обсязі володіє навчальним матеріалом, вільно самостійно та аргументовано його викладає під час усних виступів та письмових відповідей, глибоко та всебічно розкриває зміст теоретичних питань та лабораторних завдань, використовуючи при цьому обов’язкову та додаткову літературу. Правильно вирішив усі тестові завдання.
80%	Достатньо повно володіє навчальним матеріалом, обґрунтовано його викладає під час усних виступів та письмових відповідей, в основному розкриває зміст теоретичних питань та лабораторних завдань, використовуючи при цьому обов’язкову літературу. Але при викладанні деяких питань не вистачає достатньої глибини та аргументації, допускаються при цьому окремі несуттєві

	неточності та незначні помилки. Правильно вирішив більшість тестових завдань
60%	В цілому володіє навчальним матеріалом викладає його основний зміст під час усних виступів та письмових відповідей, але без глибокого всебічного аналізу, обґрунтування та аргументації, без використання необхідної літератури допускаючи при цьому окремі суттєві неточності та помилки. Правильно вирішив половину тестових завдань.
40%	Не в повному обсязі володіє навчальним матеріалом. Фрагментарно, поверхово (без аргументації та обґрунтування) викладає його під час усних виступів та письмових відповідей, недостатньо розкриває зміст теоретичних питань та лабораторних завдань, допускаючи при цьому суттєві неточності, правильно вирішив меншість тестових завдань.
20%	Частково володіє навчальним матеріалом не в змозі викласти зміст більшості питань теми під час усних виступів та письмових відповідей, допускаючи при цьому суттєві помилки. Правильно вирішив окремі тестові завдання.
0%	Не володіє навчальним матеріалом та не в змозі його викласти, не розуміє змісту теоретичних питань та практичних завдань. Не вирішив жодного тестового завдання.
ОСНОВНІ ПОЛОЖЕННЯ, ЩО РЕГЛАМЕНТУЮТЬ ОСВІТНІЙ ПРОЦЕС	
діючі положення	https://knute.edu.ua/blog/read/?pid=44402
нормативно-правова база організації освітнього процесу	https://knute.edu.ua/blog/read/?pid=7330&uk
студенту	https://knute.edu.ua/#forstudent
НЕФОРМАЛЬНА ОСВІТА Рекомендовані сертифікаційні програми, курси, посібники користувача	
Securing Software, Data and End Points	https://www.coursera.org/learn/sscp-4th-ed-course-4
Безпечні практики кодування	https://www.coursera.org/specializations/secure-coding-practices
ПОЛІТИКА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ:	
Відвідування лекційних та лабораторних занять: відвідування	Відвідування лекційних та лабораторних занять є обов'язковим. Допускаються пропуски занять з таких поважних причин, як хвороба (викладачу надається копія довідки від медичного закладу), участь в олімпіаді, творчому конкурсі тощо за попередньою домовленістю та згодою викладача за умови дозволу деканату (надаються документи чи інші матеріали, які підтверджують заявлену участь у діяльності студента).

Відпрацювання пропущених занять:	відпрацювання пропущених занять є обов'язковим незалежно від причини пропущеного заняття. Лекційне заняття має бути відпрацьоване до наступної лекції на консультації викладача з використанням ПЗ 365 Office Teams. Відпрацювання лекційного матеріалу передбачає вивчення пропущеного теоретичного матеріалу та складання тесту за цим матеріалом. Лабораторне заняття відпрацьовується під час консультації викладача (розклад консультацій на сайті).
Правила поведінки під час занять	обов'язковим є дотримання техніки безпеки в комп'ютерних лабораторіях. Студенти повинні приймати активну участь в обговоренні навчально матеріалу ознайомившись з ним напередодні (навчальний матеріал надається викладачем). Мобільні пристрої дозволяється використовувати лише під час он-лайн тестування та підготовки практичних завдань в процесі заняття. Задля зручності, дозволяється використання ноутбуків та інших електронних пристроїв під час навчання в комп'ютерних аудиторіях (за взаємною згодою всіх учасників освітнього процесу)
Політика академічної доброчесності ДТЕУ	https://knute.edu.ua/blog/read/?pid=38987&uk