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

МОНІТОРИНГ ТА ТЕСТУВАННЯ СИСТЕМ КІБЕРБЕЗПЕКИ /
MONITORING AND TESTING OF CYBERSECURITY SYSTEMS

СИЛАБУС/
SILABUS

ЗАТВЕРДЖЕНО
засіданням кафедри
(протокол №. 1
від «04» серпня 2024 р.)
завідувач кафедри
_____Олена КРИВОРУЧКО

Київ 2024

Назва освітньої компоненти	**МОНІТОРИНГ ТА ТЕСТУВАННЯ СИСТЕМ КІБЕРБЕЗПЕКИ** / MONITORING AND TESTING OF CYBERSECURITY SYSTEMS
Спеціальність	125 «Кібербезпека та захист інформації»
Освітній ступінь	Другий (магістерський)
Освітньо-професійна програма	**БЕЗПЕКА СИСТЕМ ЕЛЕКТРОННИХ КОМУНІКАЦІЙ В ЕКОНОМІЦІ**
	Лектор: **Хохлачова Юлія** -професор кафедри інженерії програмного забезпечення та кібербезпеки -кандидат технічних наук -професор Резюме викладача: https://knute.edu.ua/blog/read/?pid=48259 е-пошта: y.khokhlachova@knute.edu.ua
Консультації	https://knute.edu.ua/blog/read/?pid=47103&uk
Програма освітньої компоненти	https://knute.edu.ua/blog/read/?pid=48216
ЗМІСТ ОСВІТНЬОЇ КОМПОНЕНТИ	
Тема 1. Предмет дисципліни, її цілі.	Основні види документів. Визначення режиму доступу до інформації згідно Закон України "Про інформацію". Законодавчі акти і нормативні документи щодо захисту інформації. Закон України „Про інформацію”. Закон України „Про науково-технічну інформацію”. Закон України „Про телекомунікації”. Закон України „Про Національний архівний фонд та архівні установи”. Закон України „Про державну таємницю”.
Тема 2. Основні терміни та визначення.	Визначення термінів. Об'єкти захисту. Суб'єкти відносин. Право власності на інформацію в системі. Доступ до інформації. Відносини між суб'єктами в процесі обробки інформації в системі.
Тема 3. Організація захисту інформації в системі.	Основні питання та організаційні особливості. Відповідальність за порушення законодавства у сфері захисту інформації в системі. Міжнародне співробітництво у сфері захисту інформації в системі.
Тема 4. Поняття	Поняття моніторингу. Можливі цілі моніторингу. Різновиди

моніторингу.	моніторингу. Предмет спостережень. Поняття події.
Тема. 5. Характеристики та види подій при моніторингу.	Статистичні і сукупні характеристики подій. Види подій, що реєструються при моніторингу. Види показників спостережуваних подій. Поняття та види порогів.
Тема 6. Види моніторингу та основні питання.	Стратегічний моніторинг. Основні об'єкти стратегічного моніторингу. Оперативний моніторинг. Аналіз даних оперативного моніторингу. Моніторинг масової активності. Основні показники та цілі моніторингу масової активності. Моніторинг установ. Цілі моніторингу установ.
Тема 7. Сучасні методи та технології моніторингу.	Радіомоніторинг, його завдання та категорії вирішення завдань. Основні складові радіомоніторингу. Контент-моніторинг. Сучасні методи контент-моніторингу. Технологія TextMining. Моніторинг соціальних медіа. Моніторинг в Інтернеті. Класифікатор пошукових засобів в мережі Інтернет. Інформаційно-аналітичні системи в Інтернет. Небезпека Інтернету як джерела інформації для розвідки (моніторингу).
Тема 8. Прогнозування (передбачення). Загальні питання.	Процес прогнозування, його види та методи. Способи передбачення (прогнозування). Компоненти системи прогнозування. Методи неформальної прогнозування. Правила складання прогнозів. Задачі прогнозування в інформаційно-аналітичній роботі.
Тема 9. Підходи та методи моніторингу.	Підхід до програмної реалізації агресивності програмних засобів. Концепція безпеки програмного засобу та її властивості. Підходи до відновлення алгоритмів. Методи визначення факта інформаційного вторгнення.
Тема 10. Методи тестування криптографічних програмних систем.	Структурний метод (метод білого або скляного ящика). Поведінковий метод «чорного ящика». Метод регресивного тестування. Метод «сірого ящика». Метод дослідної експлуатації. Тестування ергономічності.
Тема 11. Основні принципи процесу тестування.	Основні принципи тестування. Їх концепції та підходи. Рівні та принципи тестування програмного забезпечення. Планування тестування. Підготовка. Тестування. Аналіз результатів тестування.
Тема 12. Методика забезпечення якості програмного забезпечення	Основні поняття та визначення. Міжнародні стандарти. Методи визначення якості програмного забезпечення. Сучасні програмні засоби для визначення якості програмного

	забезпечення. Характеристики якості ПЗ. Моделі якості ПЗ. Рекомендації та метрики с забезпечення якості.

СПИСОК ОСНОВНИХ РЕКОМЕНДОВАНИХ ДЖЕРЕЛ

1. Хохлачова Ю.Є. Моніторинг та тестування систем кібербезпеки: лабораторний практикум / Ю.Є. Хохлачова, В.М. Кінзерявий, В.В. Погорелов та ін. К.: НАУ, 2022. 56 с.
2. Браіловський М.М., Зибін С.В., Пискун І.В., Хорошко В.О., Хохлачова Ю.Є. Технології захисту інформації. К.: ЦП «Компринт», 2021. 296 с.
3. Луцький М.Г., Хорошко В.О., Хохлачова Ю.Є., Козловський В.В., Баланюк Ю.В., Прав Ю.Г. Новітні технології захисту інформації: підручник. К.: НАУ, 2023. 312 с.
4. Пирцхалава Л.Г., Хорошко В.О., Хохлачова Ю.Є., Шелест М.Є. Інформаційно-аналітичне забезпечення безпеки. – Київ: ФЛП Ямчинський О.В. 2021. 470 с.
5. *Безпека інформаційних систем: навч. посіб. / В. І. Пашорін, Ю. В. Костюк. – Київ: Держ. торг.-екон. ун-т, 2022. – 376 с..*

РЕЗУЛЬТАТИ ВИВЧЕННЯ ОСВІТНЬОЇ КОМПОНЕНТИ

Дисципліна забезпечує оволодіння здобувачами вищої освіти загальними та фаховими компетентностями і досягнення ними програмних результатів навчання:

ЗК-01.	Здатність застосовувати знання у практичних ситуаціях.
ЗК-03.	Здатність до абстрактного мислення, аналізу та синтезу.
ЗК-04.	Здатність оцінювати та забезпечувати якість виконуваних робіт.
СК-01.	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.
СК-02.	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.
СК-03.	Здатність досліджувати, розробляти і супроводжувати методи та засоби інформаційної безпеки та/або кібербезпеки на об’єктах інформаційної діяльності та критичної інфраструктури.
СК-09.	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.
СК-11.	Здатність аналізувати електронні комунікаційні мережі та протистояти діям, що становлять загрозу доступності, цілісності чи

	конфіденційності таких мереж і послуг, а також даних, що зберігаються, передаються чи обробляються, та пов'язаних із ними послуг, зокрема в економіці.
СК-12.	Здатність виконувати обов'язки внутрішнього консультанта і радника у своїй експертній області.
СК-13.	Здатність проводити дослідно-експериментальну роботу щодо процедури сканування вразливостей та їх розпізнавання в системах безпеки.
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.
РН 06	Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення.
РН-14	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.
РН-15	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.
РН-23	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.

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	Кумулятивний відсоток отриманих прохідних балів

	балів	
90-100	20	20
82-89	10	зо
75-81	20	50
69-74	10	60
60-68	40	100

Розподіл 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	4	Самостійна робота 7	2
Лабораторна робота 8	4	Самостійна робота 8	3
Лабораторна робота 9	4	Самостійна робота 9	3
Лабораторна робота 10	4	Самостійна робота 10	3
Лабораторна робота 11	4	Самостійна робота 11	3
Лабораторна робота 12	4	Самостійна робота 12	2
Додаткові бали + Захист проєкту	20	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	
European Union Agency for Cybersecurity (Агентство Європейського Союзу з питань кібербезпеки)	https://www.enisa.europa.eu
The EU Cyberdiplomacy	https://www.cyber-diplomacy-toolbox.com/

Toolbox	
MS AZURE	https://learn.microsoft.com/uk-ua/training/azure/
Cloud Native Computing Foundation	https://www.cncf.io/
Isaca	https://www.isaca.org/training-and-events
CSA (Cloud security alliance)	https://cloudsecurityalliance.org/research/artifacts
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