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

АНАЛІЗ ЗАГРОЗ ТА ЕКСПЛУАТАЦІЇ УРАЗЛИВОСТЕЙ /
ANALYSIS OF THREATS AND EXPLOITATION OF VULNERABILITIES

СИЛАБУС/
SILABUS

ЗАТВЕРДЖЕНО
засіданням кафедри
(протокол №. 1
від «07» серпня 2024 р.)
завідувач кафедри
_____Олена КРИВОРУЧКО

Київ 2024

Назва освітньої компоненти	**АНАЛІЗ ЗАГРОЗ ТА ЕКСПЛУАТАЦІЇ УРАЗЛИВОСТЕЙ** / ANALYSIS OF THREATS AND EXPLOITATION OF VULNERABILITIES
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. Національна база даних уразливостей (National Vulnerability Database)	Поняття База National Vulnerability Database. Протокол автоматизації контенту безпеки – Security Content Automation Protocol (SCAP).
Тема 2. Протоколи документування, відстеження та спільного використання інформації про інциденти	Протоколи документування та спільного використання структурної інформації про загрози. Threat Analysis Automation Protocol (TAAP), основні компоненти. Event Management Automation Protocol (EMAP) – протокол для звітів про події безпеки, основні складові. Incident Tracking and Assessment Protocol (ITAP) – протокол для відстеження, документування, управління та спільного використання інформації про інциденти, основні компоненти.
Тема 3. Банк даних загроз безпеки інформації.	Відомості про загрози ІБ та уразливості ПЗ. Основні параметри загроз та уразливостей.
Тема 4. Калькулятор	Аналіз на сайті бази даних безпеки інформації калькулятора

CVSS v2.0.	CVSS v2.0. Історія та основні параметри. Формули для розрахунку калькулятора CVSS v2.0. Приклади та застосування. Критика та порівняння версій стандарту. Приклади уразливостей з рахунком 10,0.
Тема 5. База даних уразливостей від відкритих джерел (Open Sourced Vulnerability Database).	Історія виникнення та мета проєкту. Основні відомості про базу уразливостей від відкритих джерел. Опис уразливості, що заноситься в OSVDB. Інтерфейс OSVDB.
Тема 6. Сучасні бази даних атак та їх використання в системах виявлення вторгнень.	Бази даних атак та їх структура. Набір даних NSL-KDD. База даних All.Net Security. Набір даних UNSW-NB15. Набори даних ADFA-LD та ADFA-WD.
Тема 7. База даних інцидентів веб-хакерства.	Основні питання щодо баз даних інцидентів веб-хакерства. Приклади та можливі варіанти захисту від злому. База даних інцидентів веб-хакерства The Web Hacking Incident Database (WHID).
Тема 8. Бази даних атак, сформовані при проведенні конкурсів з кібербезпеки.	Основні відмінності та особливості баз даних атак. Складові частини. Переваги та недоліки. Особливості баз даних атак та їх використання в сучасних системах виявлення вторгнень.
Тема 9. База даних уразливостей IBM X-Force.	Історія виникнення. Складові частини. Основні відомості про базу даних уразливостей IBM X-Force. Процес доступу. Приклад опису уразливості Microsoft Excel Remote Code Execution.
Тема 10. База даних записів уразливостей US-CERT	Основні відомості про базу даних записів уразливостей US-CERT. Історія виникнення та розробки. Ідентифікатор «VU #». Основні пункти опису уразливостей. Відмінності від інших баз даних. Переваги та недоліки.
Тема 11. Бази даних уразливостей в VND.	Основні пункти опису уразливості в VND. Приклад опису уразливостей. Вільні дані оцінок CVSS. Історія, термінологія. Базові показники: вектор доступу, складність доступу, автентифікація. Методи впливу: конфіденційність, цілісність, доступність. Розрахунки, приклади. Темпоральні метрики та метрики середовища. Порівняння та критика версії 2 та версії 3.
Тема 12. База даних уразливостей	Історія виникнення та основні відомості. Вміст та особливості. Дослідження бази даних уразливостей SecurityFocus.

SecurityFocus.	Візуалізація та огляд інтерфейсу. Приклад опису уразливості Bugtraq 77270.
Тема 13. Бази шаблонів атак KDD-99.	Категорування баз даних на основі принципів теорії подібності. Опис параметрів мережевого з'єднання за базою шаблонів атак KDD-99. Структура шаблонів нормальної поведінки та кібератак за базою KDD Cup 1999.
Тема 14. Бази шаблонів атак CAPEC.	Структура бази CAPEC. Загальний перелік та класифікація комп'ютерних атак бази шаблонів атак CAPEC. Порівняльний аналіз баз шаблонів. Узагальнена схема формування джерел первинних даних для розроблення шаблонів потенційно небезпечних КбА.

СПИСОК ОСНОВНИХ РЕКОМЕНДОВАНИХ ДЖЕРЕЛ

1. 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.
2. М.М. Браіловський, Н.С. Вишневська, В.Д. Козюра, Ю.В. Пепа, В.О. Хорошко, Ю.Є. Хохлачова. Комп'ютерні технології: навчальний посібник. К.: ФОП Ямчинський О.В., 2023. 200 с.
3. Браіловський М.М., Зибін С.В., Кобозєва А.А., Хорошко В.О., Хохлачова Ю.Є. Аналіз кіберзахищеності інформаційних систем Київ: ФОП Ямчинський О.В. 2021. 360 с.
4. *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:

КЗ-01.	Здатність застосовувати знання у практичних ситуаціях.
КЗ -02.	Здатність проводити дослідження на відповідному рівні.
КЗ -03.	Здатність до абстрактного мислення, аналізу та синтезу.
КЗ -04.	Здатність оцінювати та забезпечувати якість виконуваних робіт.
КЗ -05.	Здатність спілкуватися з представниками інших професійних груп різного рівня (з експертами з інших галузей знань / видів економічної діяльності).
КЗ -06.	*Здатність діяти соціально відповідально та громадсько свідомо.*
КЗ -07.	*Здатність до адаптації та дії у новій ситуації.*
КФ-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.
КФ -03.	Здатність досліджувати, розробляти і супроводжувати методи та засоби інформаційної безпеки та/або кібербезпеки на об’єктах інформаційної діяльності та критичної інфраструктури.
КФ -05.	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.
РН-5	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-6	Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення.
РН-10	Забезпечувати безперервність бізнес/операційних процесів, а також виявляти уразливості інформаційних систем та ресурсів, аналізувати та оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації.
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	Відсоток балів відносно	Кумулятивний відсоток

ДТЕУ	загальної кількості одержаних прохідних балів	отриманих прохідних 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	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
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	https://www.enisa.europa.eu

Cybersecurity (Агентство Європейського Союзу з питань кібербезпеки)	
The EU Cyberdiplomacy Toolbox	https://www.cyber-diplomacy-toolbox.com/
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