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

ОСНОВИ КІБЕРБЕЗПЕКИ / CYBERSECURITY ESSENTIALS

СИЛАБУС/
SILABUS

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

Київ 2024

Назва освітньої компоненти	**ОСНОВИ КІБЕРБЕЗПЕКИ / CYBERSECURITY ESSENTIALS**
Спеціальність	121 «Інженерія програмного забезпечення»
Освітній ступінь	бакалавр / bachelor
Освітньо-професійна програма	**Інженерія програмного забезпечення / Software Engineering**
	Лектор: **Горохова Олена** -доцент кафедри інженерії програмного забезпечення та кібербезпеки - кандидат фізико-математичних наук - доцент Резюме викладача: https://knute.edu.ua/blog/read/?pid=48292 Науковий профіль: https://knute.edu.ua/blog/read/?pid=46703&uk e-пошта: o.horokhova@knute.edu.ua
Консультації	https://knute.edu.ua/blog/read/?pid=47103&uk
Програма освітньої компоненти	https://knute.edu.ua/blog/read/?pid=48212
ЗМІСТ ОСВІТНЬОЇ КОМПОНЕНТИ	
Тема 1. Кіберпростір і кібербезпека — головні ознаки нової інформаційної цивілізації	Поняття інформаційна безпека, кібербезпека, кіберпростір, кіберборотьба, кібертероризм, кіберзброя. Кіберпростір як сфера ведення війн сучасності та майбутнього. Сутність кібербезпеки інформаційного суспільства. Кіберінциденти: передумови скоєння та наслідки. Дії у кіберпросторі та їх особливості. Класифікація форм і способів кібердій. Основи кіберрозвідки. Основи кіберзахисту. Огляд областей кібербезпеки. Приклади доменів кібербезпеки. Зростання кібер-доменів. Поняття «кіберзлочинець» та мотиви кіберзлочинів. Класифікація зловмисників.
Тема 2. Національна система кібербезпеки України	Основні положення Стратегії кібербезпеки України. Сутність та завдання Національної системи забезпечення кібербезпеки України Пріоритети та напрями забезпечення кібербезпеки України згідно з чинним законодавством. Захист відкритої інформації в державних органах. Компетенція органів державної влади, органів місцевого самоврядування та їх посадових осіб у сфері охорони державної таємниці. Правове забезпечення у сфері інформаційної безпеки та кібербезпеки. Структура національної безпеки України. Суб'єкти забезпечення інформаційної безпеки як складової національної безпеки України. Основні пріоритети забезпечення інформаційної безпеки.
Тема 3.	Модель кібербезпеки ISO. Огляд моделі. Галузі кібербезпеки.

Сутність та основні процедури керування кібербезпекою	Цілі контролю. Контроль. Використання моделі ISO для кібербезпеки. Модель кібербезпеки ISO та тріада КЦД. Модель кібербезпеки ISO і можливі стани даних. Модель кібербезпеки ISO і технології захисту.
Тема 4. Кібератаки, загрози та їх властивості. Характеристика сучасних кібератак	Комп'ютерні атаки та технології їхнього виявлення. Сутність та класифікація кібератак. Етапи реалізації атак. Відмова в обслуговуванні. Аналіз трафіку (Sniffing). Підміна. Man-in-the-middle. Атаки нульового дня. Клавіатурні шпигуни (кейлогери). Захист від атак. Атаки на бездротові мережі та мобільні пристрої. Grayware та SMiShing. Несанкціоновані точки доступу. Глушіння радіочастот (RF Jamming). Bluejacking та Bluesnarfing. Атаки на WEP та WPA. Захист від атак на бездротові мережі та мобільні пристрої.Атаки на застосунки. Міжсайтовий скриптинг. Ін'єкція коду. Переповнення буфера. Віддалений запуск програм. Захист від атак на застосунки. Атака "Відмова в обслуговуванні" (DoS). Розподілена DoS атака (Distributed DoS Attack, DDoS). Отруєння SEO.Зміст, класифікація та ознаки кіберзагроз. Основні характеристики кіберзагроз. Внутрішні та зовнішні кіберзагрози. Кіберзагрози через Інтернет-сервіси. Поширення кіберзагроз. Кіберзагрози підвищеної складності.
Тема 5. Дезінформація як елемент кібератак. Сценарії розвитку та методи протидії	Поняття «дезінформації». Канали поширення дезінформації. Типи неправдивої інформації. Технології неправдивих повідомлень. Інструменти виявлення неправдивих повідомлень. Види маніпуляцій. Маніпуляції з медіаданими. Маніпулювання новинами. Маніпулювання експертними оцінками. Маніпулювання повідомленнями. Маніпуляції з результатами досліджень. Пропаганда як інструментів інформаційного впливу. Способи протидії неправдивим повідомленням.
Тема 6. Комп’ютерна вірусологія	Загальні поняття про комп’ютерні віруси, історія їх виникнення та розвитку. Загальні принципи функціонування комп’ютерних вірусів, їх розмноження. Класифікація комп’ютерних вірусів і принципи її побудови. Алгоритми роботи вірусів. Файлові, завантажувальні (бутові) та файлово-завантажувальні віруси. Макровіруси та мережні віруси. Класифікаційний код вірусу. Резидентність, використання стелсалгоритмів, самошифрування та поліморфізм, використання нестандартних методів. Шляхи розповсюдження шкідливого програмного забезпечення (ШПЗ), вектори атак. Типи шкідливого програмного забезпечення. Шпигунські програми (spyware). Симптоми зараження ШПЗ. Завантажувач (дропер/лоадер). Викрадач інформації «інфостілер або стілер». Keylogger “кейлогер”. «JS-сніфери». Троянські програми віддаленого доступу .rat. Банківські трояни (banking trojans). Ransomware (програма-вимагач, програма-шантажист). Майнери (miners). Шкідливе програмне

	забезпечення для знищення інформації без можливості її відновлення. Рекламне шкідливе програмне забезпечення (adware).
Тема 7. Соціальна інженерія	Поняття соціальної інженерії. Методи соціальної інженерії. Види атак соціальної інженерії. Претекстінг (pretexting). Тейлгейтінг (tailgating). Послуга за послугу (quid pro quo). Злам пароля WI-FI. Атаки грубої сили (brute-force attacks). Прослуховування мережі (network sniffing). Фішингова атака. Етапи атаки із використанням СІ. Розвідка та збір інформації із відкритих джерел. Легендування та планування атаки із використання методів СІ. Використання вразливостей як розповсюджений метод проникнення для отримання інформації.
Тема 8. Соціотехнічна безпека: проблемні аспекти	Соціальна інженерія як метод розвідки складних соціальних і соціотехнічних систем: основні аспекти, поняття та визначення. Особливості захисту сучасної інфосфери в умовах стороннього кібернетичного впливу. Соціальний фактор у проблемі забезпечення інформаційної і кібербезпеки. Соціальні мережі: особливості, основні поняття та визначення. Моніторинг соціальних мереж − цілі та способи реалізації. Поняття соціотехнічної системи та її властивостей. Системний підхід як загальнометодологічний принцип створення складних соціотехнічних систем.
Тема 9. Безпека спілкування в кіберпросторі	Захист інформації в глобальних мережах. Характер проведення атак у глобальних мережах. Захист під час використання WWW (World Wide Web).Безпечне користування мережею «Інтернет». Найпоширеніші способи нелегального заробітку в мережі «Інтернет». Безпека браузерів. Безпека даних. Безпечне користування мережами WI-FI. Основні правила безпечного користування WI-FI. Безпечне користування месенджерами.
Тема 10. Особливості економічної діяльності суб'єктів господарювання в кіберпросторі	Безпека користування соціальними мережами. Реєстрація. Стійкий пароль. Оновлення паролів та парольних фраз. Конфіденційність даних. Налаштування конфіденційності та інших питань безпеки. Безпека мобільних пристроїв. Блокування доступу до пристрою. Безпечна робота в мультимедійних засобах спілкування. Передавання вживаних мобільних пристроїв іншим особам. Передавання контактної інформації іншим особам. Вірусне програмне забезпечення. Додаткові функції мобільного пристрою. Головні правила роботи з мобільними пристроями. Безпека користування електронною поштою. Конфіденційність електронної пошти. Найвідоміші атаки через електронну пошту. Загрози під час користування поштовою скринькою. Легітимні та фішингові листи (investigation). Забезпечення безпеки особистої поштової скриньки (рекомендації).
Тема 11.	Технічні канали витоку інформації. Способи несанкціонованого

Безпека цифрового простору суб'єктів господарювання	зняття інформації з технічних каналів її витоку. Класифікація каналів витоку інформації. Методи та засоби блокування технічних каналів витоку інформації. Системи та засоби виявлення, пошуку та знешкоджування технічних засобів зняття інформації. Захист акустичної інформації від зняття радіопристроями. Захист інформації від витоку по технічних каналах, утворених допоміжними технічними засобами. Захист інформації від несанкціонованого запису звукозаписувальними пристроями. Захист електронної інформації. Захист письмової інформації від оптичного зняття.
Тема 12. Безпека Інтернету-речей	Історія Інтернету-речей. Екосистема Інтернету-речей. Архітектура Інтернету-речей. Технології Інтернету-речей. «Розумний та безпечний будинок». Анатомія кібератак на IoT-пристрої. Mirai. Stuxnet. Ланцюжкова реакція. Туманні технології. Криптографія. Симетрична криптографія. Асиметрична криптографія. Криптографічний хеш (аутентифікація і цифровий підпис). Інфраструктура відкритого ключа. Блокчейн і криптовалюта в Інтернеті-речей. Рекомендації щодо захисту IoT-пристроїв.
Тема 13. Системи захисту інформації на проникнення	Технології захисту на основі програмного забезпечення. Апаратні засоби захисту. Мережні технології захисту. Хмарні технології захисту. Фізична безпека. Загрози, пов'язані з недотриманням правил фізичної безпеки. Найпопулярніша атака через фізичне втручання: Stuxnet. Захист інформації за допомогою міжмережних екранів. Маскування даних. Технології маскування даних. Стеганографія, основні терміни та визначення. Історичні приклади стеганосистем. Галузі застосування стеганографії. Методи та моделі стеганографії. Комп'ютерна і цифрова стеганографія, цифрові водяні позначки. Практичні аспекти побудови стеганосистем. Приховування даних у текстових файлах: методи текстової стеганографії; аналіз реалізації методів.
Тема 14. Основні методи забезпечення кібербезпеки суб'єкта господарювання	Типи контролю доступу. Контроль фізичного доступу. Системи розмежування логічного доступу. Адміністративний контроль доступу. Стратегії контролю доступу. Дискреційне розмежування доступу. Контроль доступу на основі ролей. Розмежування доступу на основі правил. Ідентифікація. Управління ідентифікацією та доступом. Методи аутентифікації. Багатофакторна аутентифікація. Аутентифікація на основі одноразових паролей. Строга аутентифікація. Криптографічні протоколи строгої аутентифікації. Біометрична аутентифікація користувача. Авторизація. Використання авторизації. Типи засобів контролю безпеки. Превентивні засоби контролю. Стримуючі засоби контролю. Ефективні механізми розкриття порушень. Коригуючі засоби контролю. Засоби відновлення. Компенсуючі засоби контролю.

	Криптографія і її основні поняття. Модель криптографічної системи. Принцип Керкхоффса. Етапи розвитку криптографічних систем. Види історичних шифрів. Типи шифрування. Шифрування за допомогою закритого ключа. Процес симетричного шифрування. Типи криптографічних перетворень. Симетричні криптосистеми шифрування. Алгоритм шифрування DES, 3-DES. Стандарт шифрування AES. Основні режими роботи блочного симетричного алгоритму.

СПИСОК ОСНОВНИХ РЕКОМЕНДОВАНИХ ДЖЕРЕЛ

1. Даник Ю.Г. Основи кібербезпеки та кібероборони: підручник / Ю.Г. Даник, П.П. Воробієнко, В.М. Чернега. – [Видання друге, перероб. та доп.]. – Одеса.: ОНАЗ ім. О.С. Попова, 2019. − 320 с. ISBN 978-617-582-069-8
2. Бурячок В.Л. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / [В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко, С. В. Толюпа]; за заг. ред. д-ра техн. наук, професора В. Б. Толубка.− К.: ДУТ, 2015.− 288 с.
3. Безпека інформаційних систем: навч. посіб. / В. І. Пашорін, Ю. В. Костюк. – Київ: Держ. торг.-екон. ун-т, 2022. – 376 с.
4. Гребенюк А.М. Основи управління інформаційною безпекою: навч. посібник / А.М. Гребенюк, Л.В. Рибальченко. Дніпро: Дніпроп. держ. унт внутріш. справ, 2020. – 144 с.

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 застосовувати знання у практичних ситуаціях.
ЗК03.	Здатність спілкуватися державною мовою як усно, так і письмово.
ЗК04.	Здатність спілкуватися іноземною мовою як усно, так і письмово.
ЗК05.	Здатність вчитися і оволодівати сучасними знаннями
ЗК06.	Здатність до пошуку, оброблення та аналізу інформації з різних джерел.
ЗК13.	Здатність здійснювати професійну діяльність у відповідності з чинними нормативними і правовими актами.
СК14.	Здатність ідентифікувати, класифікувати та формулювати вимоги до програмного забезпечення.
СК18.	Здатність дотримуватися специфікацій, стандартів, правил і рекомендацій в професійній галузі при реалізації процесів життєвого циклу.
СК19.	Здатність аналізувати, вибирати і застосовувати методи і засоби для забезпечення інформаційної безпеки (в тому числі кібербезпеки).
СК21.	Здатність застосовувати фундаментальні і міждисциплінарні знання для успішного розв’язання завдань інженерії програмного забезпечення.
РН01.	Аналізувати, цілеспрямовано шукати і вибирати необхідні для вирішення професійних завдань інформаційно-довідникові ресурси і знання з урахуванням сучасних досягнень науки і техніки.
РН04.	Знати і застосовувати професійні стандарти і інші нормативно-правові документи в галузі інженерії програмного забезпечення.

РН09.	Знати та вміти використовувати методи та засоби збору, формулювання та аналізу вимог до програмного забезпечення.

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	30
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	5	Самостійна робота 1	5
Лабораторна робота 2	5	Самостійна робота 2	5
Лабораторна робота 3	5	Самостійна робота 3	5
Лабораторна робота 4	5	Самостійна робота 4	5
Лабораторна робота 5	5	Самостійна робота 5	5
Лабораторна робота 6	5	Самостійна робота 6	5
Лабораторна робота 7	5		
Лабораторна робота 8	5		
Лабораторна робота 9	5		
Лабораторна робота 10	5		
Лабораторна робота 11	5		
Лабораторна робота 12	5		
		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	
Cybersecurity	https://skillsbuild.org/uk/students/course-catalog/cybersecurity

Безпека в інтернеті під час війни: практичний курс	https://prometheus.org.ua/course/course-v1:MINZMIN+ISWT101+2023_T2
Цифрова безпека на персональному рівні	https://prometheus.org.ua/course/course-v1:Prometheus+DSPL101+2023_T1
Цифрова безпека для громадських організацій в умовах війни	https://prometheus.org.ua/course/course-v1:Prometheus+DSPO101+2023_T1
Медіаграмотність: як не піддаватися маніпуляціям?	https://prometheus.org.ua/course/course-v1:Prometheus+MEDIA_L101+2022_T3
Інформаційна гігієна під час війни	https://prometheus.org.ua/course/course-v1:Prometheus+IHWAR101+2022_T2
Інформаційна безпека	https://prometheus.org.ua/course/course-v1:Internews+INFOS101+UA_2021_T3
Інформаційна гігієна. Як розпізнати брехню в соцмережах, в інтернеті та на телебаченні	https://prometheus.org.ua/course/course-v1:Prometheus+IH101+2021_T3
Дезінформація: види, інструменти та способи захисту	https://prometheus.org.ua/course/course-v1:Prometheus+DISINFO101+2021_T2
Доступ до публічної інформації: від А до Я	https://prometheus.org.ua/course/course-v1:COE+PI101+2017_T1
Кіберняні. Цифрова безпека для почвтківців: як попередити кібератаку та захищати дані в інтернеті	https://osvita.diia.gov.ua/courses/cybernanny

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