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 БЕЗПРОВОДОВИХ ТА МОБІЛЬНИХ МЕРЕЖ /
WIRELESS AND MOBILE SECURITY TECHNOLOGIES

СИЛАБУС/
SILABUS

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

Київ 2024

Назва освітньої компоненти	**ТЕХНОЛОГІЇ БЕЗПЕКИ БЕЗПРОВОДОВИХ ТА МОБІЛЬНИХ МЕРЕЖ /** WIRELESS AND MOBILE SECURITY TECHNOLOGIES
Спеціальність	125 «Кібербезпека та захист інформації»
Освітній ступінь	Другий (магістерський)
Освітньо-професійна програма	**БЕЗПЕКА СИСТЕМ ЕЛЕКТРОННИХ КОМУНІКАЦІЙ В ЕКОНОМІЦІ**
	Лектор: **Терейковський Ігор** -професор кафедри інженерії програмного забезпечення та кібербезпеки -доктор технічних наук -професор Резюме викладача: https://hait.od.ua/index.php/journal/Tereikovskyi е-пошта: terejkowski@ukr.net
	Асистент лектора: **Шестак Ярослав** -старший викладач кафедри інженерії програмного забезпечення та кібербезпеки -Директор ІОЦ - ГЦІТ ДТЕУ Резюме викладача: https://knute.edu.ua/blog/read/?pid=43517&uk 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=48216

ЗМІСТ ОСВІТНЬОЇ КОМПОНЕНТИ

Тема 1. Основи теорії безпроводової передачі. Загрози, атаки та захист безпроводових мереж	Безпроводові мережі та їх класифікація. Технології побудови безпроводових мереж. Дослідження безпроводових мереж. Огляд основних протоколів бездоротових мереж. Класифікація атак на безпроводові мережі та їх характеристики. Моделі та критерії загроз безпроводових мереж. Методи оцінки загроз та атак на безпроводові мережі. Розгортання робочого середовища для проведення аудиту безпеки безпроводових мереж.
Тема 2.	Дослідження безпроводових мереж та їх протоколів.

Мережеві прото-коли та служби безпроводових мереж	Мережеві служби. Вивчення основних мережевих протоколів та принципів їх роботи. Маршрутизація в безпроводових мережах. Вибір маршрутів та ретрансляція пакетів.
Тема 3. Стандарти мереж мобільного зв'язку. Загрози та вразливості мо-більних пристроїв	Стандарти мереж мобільного зв'язку. Базові технології бездротового зв'язку. Класифікація загроз та вразливостей мобільних пристроїв. Управління з метою забезпечення захисту мобільного зв'язку. Життєвий цикл рішень з безпеки мобільних пристроїв. Сканування мережевих протоколів.
Тема 4. Архітектура безпроводових мереж 4G та 5G. Загрози та вразливості стандартів 3G, 4G, 5G	Архітектура побудови мереж LTE. Протоколи передачі даних в LTE. Стандарти безпеки при побудові LTE. Архітектура безпеки LTE. Дослідження основних аспектів стандарту безпеки LTE. Аналіз архітектури безпеки EPS.
Тема 5. Архітектура WiFi-технологій. Загрози та вразливості WiFi-мереж	Стандарти WiFi. Протоколи безпеки WPA та WPA2, RADIUS та EAP. Визначення та розуміння впливу корпоративних стандартів безпеки, включаючи: 802.11x. Класифікація та особливості мобільних ad-hoc мереж. Сенсорні та MANET мережі. Класифікація загроз і вразливостей Wi-Fi-мереж та мобільних додатків. Методи захисту Wi-Fi-мереж.
Тема 6. Моніторинг без-пеки безпрово-дових мереж	Класифікації мережевих атак та дослідження методів протидії і захисту. Дослідження та моніторинг систем реагування на інциденти. Захист від мережевих атак. Реагування на інциденти та обробка результатів.
Тема 7. Шляхи захисту безпроводових мереж	Технології забезпечення об'єктивного контролю захищеності безпроводових мереж. Проведення тестування на проникнення, аналізу вразливостей. Технології підвищення захищеності безпроводових мереж.
Тема 8. Мережі широкосмугового бездпроводового доступу сімейства стандартів IEEE 802.16 (WiMAX)	Структура та особливості стандарту IEEE 802.16. Фізичний рівень та MAC-рівень стандарту IEEE 802.16. Керування з єднаннями в мережах фіксованого доступу IEEE 802.16. Mesh-мережі. Мережі WiMAX мобільного доступу IEEE 802.16e. Базова мережна модель для мобільних систем зв'язку. Попередня аутентифікація. Механізм керування потужністю. Шифрування відновлень CID. Порядок розподілу IP-адрес. Безпека мереж WiMAX.

Тема 9. Безпека безпроводових сенсорних мереж WSN	Основні поняття і принципи сенсорних мереж. Базова архітектура сенсорної мережі. Вузли бездпроводової сенсорної мережі WSN. Способи передачі даних в WSN. Протоколи і технології передачі даних в WSN. Типи вузлів WSN. Класифікація атак на WSN. Моделювання режимів протидії атакам на WSN. Моделі та методи запобігання загрозам на WSN. Безпека безпроводових сенсорних мереж.
Тема 10. Безпека персональних безпроводових мереж ZigBee	Технології ZigBee, використання та розгортання. Вибір обладнання ZigBee. Архітектура ZigBee і IEEE 802.15.4 фізичного та MAC-рівня. Механізми захисту ZigBee та IEEE 802.15.4; автентифікація та криптографічний контроль. Слабкі сторони у механізмах надання та керування ключовими інструментами ZigBee. Інструменти для підслуховування та керування мережами ZigBee. Пошук ZigBee-пристроїв за допомогою інструментів аналізу сигналу. Шифрування даних модуля ZigBee.
Тема 11. Безпека персональних безпроводових мереж Bluetooth	Технічні аспекти побудови і функціонування мереж персонального зв'язку технології Bluetooth. Стандарти Bluetooth і HomeRF. Архітектура і логічна структура мережі Bluetooth. Структура пристроїв Bluetooth. Типи антен для мереж Bluetooth. Атаки на Bluetooth. Політика безпеки персональних безпроводових мереж Bluetooth.
Тема 12. Безпека безпроводової мережі WiFi	Класифікація та вплив DoS-атак на інфраструктуру WiFi мережі. Використання безпроводового сніфінгу як механізму розуміння режиму роботи WLAN-картки. Сніфінг у керованому режимі, сніфінг в режимі монітора, переваги RFMON-сніфінгу, реалізація RFMON. Аналіз безпроводового трафіку за допомогою TCPdump, Wireshark.
Тема 13. Безпроводова система виявлення вторгнень WIDS	Класифікація систем виявлення вторгнень. Концепції IDS та WIDS. Моделі розгортання WIDS, структура та архітектура. Моніторинг безпроводових мереж за допомогою системи виявлення вторгнень WIDS.
Тема 14. Захист мереж від несанкціонованого доступу з використанням технології VPN	Види віртуальних приватних мереж. Архітектура та засоби побудови VPN. Варіанти побудови захищених каналів VPN. Сервіси безпеки мережі VPN. Протоколи VPN. Побудова захищених корпоративних мереж на основі VPN-рішення. Концепція захищених віртуальних приватних мереж. Способи утворення захищених тунелів. Рівні реалізації

	VPN. VPN на основі шифрування. Методи захисту інформації в мережах VPN.

СПИСОК ОСНОВНИХ РЕКОМЕНДОВАНИХ ДЖЕРЕЛ

1. Бурячок В.Л., Соколов В.Ю. Методи забезпечення гарантоздатності і функціональної безпеки безпроводової інфраструктури на основі апаратного розділення абонентів: навчальний посібник. Київ : КУБГ, 2019. 164 с.
2. Сайко В.Г., Казіміренко В.Я., Літвінов Ю.М. Мережі бездротового широкосмугового доступу. Навчальний посібник. – К.: ДУТ, 2015. – 196 с.
3. Інформаційна безпека: навчальний посібник / Ю.Я. Бобало, І. В. Горбатий, М.Д. Кіселичник, А.П. Бондарєв та інші; за заг. ред. д-ра техн. наук, проф. Ю.Я. Бобала та д-ра техн. наук, доц. І. В. Горбатого. – Львів : Видавництво Львівської політехніки, 2019. – 580 с.
4. *Безпека інформаційних систем: навч. посіб. / В. І. Пашорін, Ю. В. Костюк. – Київ: Держ. торг.-екон. ун-т, 2022. – 376 с.*
5. *Хорошко О.В. Захист систем електронних комунікацій: навч.посіб./ В.О. Хорошко, О.В. Криворучко, М.М. Браіловський та ін. – Київ: Київ. нац. торг.-екон. ун-т, 2019. – 164 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 -05.	Здатність спілкуватися з представниками інших професійних груп різного рівня (з експертами з інших галузей знань / видів економічної діяльності).
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 -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.
КФ -03.	Здатність досліджувати, розробляти і супроводжувати методи та засоби інформаційної безпеки та/або кібербезпеки на об’єктах інформаційної діяльності та критичної інфраструктури.
КФ -04.	Здатність аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації,

	формувати стратегію і політики інформаційної безпеки з урахуванням вітчизняних і міжнародних стандартів та вимог.
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.
КФ -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.
КФ -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.
КФ -12.	*Здатність виконувати обов'язки внутрішнього консультанта і радника у своїй експертній області.*
КФ -13.	*Здатність проводити дослідно-експериментальну роботу щодо процедури сканування вразливостей та їх розпізнавання в системах безпеки.*
РН- 01	Вільно спілкуватись державною та іноземною мовами, усно і письмово для представлення і обговорення результатів досліджень та інновацій, забезпечення бізнес\операційних процесів та питань професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.
РН-02	Інтегрувати фундаментальні та спеціальні знання для розв'язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах.
РН-04	Застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки.
РН- 08	Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/ або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури
РН- 09	Аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації на базі стратегії і політики інформаційної безпеки.
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- 11	Аналізувати, контролювати та забезпечувати ефективне функціонування системи управління доступом до інформаційних

	ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки та/або кібербезпеки організації.
РН- 13	Досліджувати, розробляти, впроваджувати та використовувати методи та засоби криптографічного та технічного захисту інформації бізнес/операційних процесів, а також аналізувати і надавати оцінку ефективності їх використання в інформаційних системах, на об'єктах інформаційної діяльності та критичної інфраструктури.
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- 17	Мати навички автономного і самостійного навчання у сфері інформаційної безпеки та/або кібербезпеки і дотичних галузей знань, аналізувати власні освітні потреби та об'єктивно оцінювати результати навчання
РН- 20	Ставити та вирішувати складні інженерно-прикладні та наукові задачі інформаційної безпеки та/або кібербезпеки з урахуванням вимог вітчизняних та світових стандартів та кращих практик
РН- 24	*Приймати обґрунтовані рішення та вживати відповідних технічних та організаційних заходів для забезпечення безпеки електронних комунікаційних мереж та послуг з метою гарантування цілісності власних електронних комунікаційних мереж, безперервності надання електронних комунікаційних послуг, недопущення несанкціонованого доступу до електронних комунікаційних мереж.*
РН- 25	*Виконувати обов'язки внутрішнього консультанта/ радника в технічній сфері та галузі авторського права щодо електронних носіїв інформації.*
РН- 27	*Проводити сканування систем безпеки інформаційних ресурсів на вразливості.*
РН- 28	*Застосовувати принципи забезпечення безпеки інформації – збереження конфіденційності, цілісності та доступності.*

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

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 Cybersecurity (Агентство Європейського Союзу з питань кібербезпеки)	https://www.enisa.europa.eu
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