КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ 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

ЗАТВЕРДЖЕНО
вченою радою КНТЕУ
(прот. п. __ від «25» 11 2021 р.)
Ректор
_____ Анатолій МАЗАРАКІ

ТЕХНОЛОГІЇ БЕЗПЕКИ БЕЗПРОВОДОВИХ ТА МОБІЛЬНИХ МЕРЕЖ /
WIRELESS AND MOBILE SECURITY TECHNOLOGIES

ПРОГРАМА/
COURSE SUMMARY

Київ 2021

Автори: Ю.В. КОСТЮК, старший викладач кафедри інженерії програмного забезпечення та кібербезпеки,
Л.О. ВЛАСЕНКО, кандидат технічних наук, доцент кафедри інженерії програмного забезпечення та кібербезпеки,
Т.В. САВЧЕНКО кандидат технічних наук, доцент кафедри інженерії програмного забезпечення та кібербезпеки, гарант освітньої програми,
М.В. САШНЬОВА, кандидат технічних наук, доцент, кафедри інженерії програмного забезпечення та кібербезпеки

Програму розглянуто і затверджено на засіданні кафедри інженерії програмного забезпечення та кібербезпеки «1» листопада 2021 р., протокол № 10.

Рецензенти: Н.О. КОТЕНКО, канд. пед. наук, доцент кафедри інженерії програмного забезпечення та кібербезпеки,
В.П. ЗВЄРЄВ, кандидат технічних наук, заступник керівника служби з питань інформаційної безпеки та кібербезпеки – керівник управління інформаційної безпеки Апарату Ради Національної безпеки і оборони України

ТЕХНОЛОГІЇ БЕЗПЕКИ БЕЗПРОВОДОВИХ ТА МОБІЛЬНИХ МЕРЕЖ /
WIRELESS AND MOBILE SECURITY TECHNOLOGIES

ПРОГРАМА /
COURSE SUMMARY

ВСТУП

Дисципліна «Технології безпеки безпроводових та мобільних мереж» є обов'язковою компонентою навчального плану підготовки студентів денної та заочної форм навчання другого (магістерського) рівня вищої освіти галузі знань 12 «Інформаційні технології», спеціальності 125 «Кібербезпека», освітньої програми «Безпека систем електронних комунікацій в економіці».

Програму підготовлено відповідно до Стандарту вищої освіти України із зазначеної спеціальності та відповідної освітньо-професійної програми підготовки магістрів КНТЕУ.

Програма складається з таких частин:

1. Мета, завдання та предмет дисципліни.
2. Передумови вивчення дисципліни як вибіркової компоненти освітньої програми.
3. Результати вивчення дисципліни.
4. Зміст дисципліни.
5. Список рекомендованих джерел.

1. МЕТА, ЗАВДАННЯ ТА ПРЕДМЕТ ДИСЦИПЛІНИ

Метою викладання навчальної дисципліни «Технології безпеки безпроводових та мобільних мереж» є формування у майбутніх спеціалістів умінь та компетенцій для оцінювання та забезпечення необхідного рівня захищеності інформації в безпроводових та мобільних мережах; уміння вирішувати задачі адміністрування безпроводових та мобільних мереж, застосовувати нормативно-правові, організаційні та технічні процедури при роботі безпроводових і мобільних технологій; надання знань з питань безпеки та захисту сучасних безпроводових та мобільних мереж; захист сучасного програмно-апаратного забезпечення безпроводових та мобільних мереж.

Завданням дисципліни є: формування теоретичних знань та практичних умінь у сфері технологій безпеки безпроводових та мобільних мереж, інформаційної та кібернетичної безпеки.

Предметом вивчення дисципліни є технології щодо здійснення професійної діяльності з питань захисту та безпеки мобільних технологій та безпроводових мереж; методи та засоби оцінювання та забезпечення необхідного рівня захищеності інформації.

2. ПЕРЕДУМОВИ ВИВЧЕННЯ ДИСЦИПЛІНИ ЯК ВИБІРКОВОЇ КОМПОНЕНТИ ОСВІТНЬОЇ ПРОГРАМИ

знання:

- інформаційних технологій;
- безпека інформаційних систем та мереж;
- іноземної мови за професійним спрямуванням;
- організації комп'ютерних мереж.

вміння: вільно працювати:

- з офісними додатками Microsoft;
- з хмарними сервісами Office 365;
- з пошуковою системою Google.

3. РЕЗУЛЬТАТИ ВИВЧЕННЯ ДИСЦИПЛІНИ

Дисципліна «Технології безпеки безпроводових та мобільних мереж» як обов'язкова компонента освітньої програми, забезпечує оволодіння студентами загальними та фаховими компетентностями і досягнення ними програмних результатів навчання за відповідною освітньо-професійною програмою:

«Безпека систем електронних комунікацій в економіці (ОС «магістр»)

Номер в освітній програмі	Зміст компетентності	Номер теми, що розкриває зміст компетентності
Загальні компетентності за освітньою програмою		
КЗ-1.	Здатність застосовувати знання у практичних ситуаціях.	1-14
КЗ-2.	Здатність проводити дослідження на відповідному рівні.	1-14
КЗ-5.	Здатність спілкуватися з представниками інших професійних груп різного рівня (з експертами з інших галузей знань / видів економічної діяльності).	1-14

Номер в освітній програмі	Зміст компетентності	Номер теми, що розкриває зміст компетентності
Спеціальні (фахові, предметні) компетентності за освітньою програмою		
КФ1.	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.	1-14
КФ2.	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.	1-14
КФ3.	Здатність досліджувати, розробляти і супроводжувати методи та засоби інформаційної безпеки та/або кібербезпеки на об’єктах інформаційної діяльності та критичної інфраструктури.	1-14
КФ4.	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.	1-14
КФ5.	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.	1-14
КФ9.	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.	1-14

Номер в освітній програмі	Зміст компетентності	Номер теми, що розкриває зміст компетентності
Програмні результати навчання за освітньою програмою		
РН1	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.	1-14
РН2	Інтегрувати фундаментальні та спеціальні знання для розв’язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах.	1-14
РН4	Застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки.	1-14
РН8	Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/ або кібербезпеки на об’єктах інформаційної діяльності та критичної інфраструктури	1-14
РН9	Аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації на базі стратегії і політики інформаційної безпеки.	1-14
РН10	Забезпечувати безперервність бізнес/операційних процесів, а також виявляти уразливості інформаційних систем та ресурсів, аналізувати та оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації.	1-14
РН11	Аналізувати, контролювати та забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки та/або кібербезпеки організації.	1-14
РН13	Досліджувати, розробляти, впроваджувати та використовувати методи та засоби криптографічного та технічного захисту інформації бізнес/операційних процесів, а також аналізувати і надавати оцінку ефективності їх вико-	1-14

Номер в освітній програмі	Зміст компетентності	Номер теми, що розкриває зміст компетентності
	ристання в інформаційних системах, на об'єктах інформаційної діяльності та критичної інфраструктури.	
РН15	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.	1-14
РН17	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	1-14
РН20	Ставити та вирішувати складні інженерно-прикладні та наукові задачі інформаційної безпеки та/або кібербезпеки з урахуванням вимог вітчизняних та світових стандартів та кращих практик	1-14

4. ЗМІСТ ДИСЦИПЛІНИ

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.

Список рекомендованих джерел:

Основний: 1 [с. 13-49], 2 [с. 7-13. 109-127], 3 [с. 373-385], 4 [с. 64-83, 92-123]

Додатковий: 5 [с. 67-95], 7 [с. 6-17, 55-96], 9 [с. 143-210], 10 [с. 59-82], 12 [с. 7-29]

Інтернет-ресурси: 13-14,18-19

Тема 2. Мережеві протоколи та служби безпроводових мереж

Дослідження безпроводових мереж та їх протоколів. Мережеві служби. Вивчення основних мережевих протоколів та принципів їх роботи. Маршрутизація в безпроводових мережах. Вибір маршрутів та ретрансляція пакетів.

Список рекомендованих джерел:

Основний: 2 [с. 109-127, 136-153, 157-174]

Додатковий: 5 [с. 67-95], 7 [22-96], 10 [с. 84-151], 12 [с. 57-115]

Інтернет-ресурси: 15-17

Тема 3. Стандарти мереж мобільного зв'язку. Загрози та вразливості мобільних 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.

Список рекомендованих джерел:

Основний: 1 [с. 101-135], 2 [с. 185-202]

Додатковий: 6 [с. 4-42], 8 [с. 22-31], 9 [с. 143-210], 12 [с. 57-115]

Інтернет-ресурси: 15-17

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.

Класифікація загроз та вразливостей 3G, 4G, 5G.

Список рекомендованих джерел:

Основний: 1 [с. 101-135], 4 [с. 64-83, 92-123]

Додатковий: 6 [с. 4-15], 8 [с. 22-53, 65-82],10 [с. 206-240], 12 [с. 57-115]

Інтернет-ресурси: 15-18

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.

Список рекомендованих джерел:

Основний: 2 [с. 157-174], 3 [с. 373-385], 4 [с. 64-83, 92-123]

Додатковий: 5-7 [с. 55-96], 10 [с. 206-240], 12 [53-67], 12 [с. 57-115]

Інтернет-ресурси: 13-19

Тема 6. Моніторинг безпеки безпроводових 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.

Список рекомендованих джерел:

Основний: 1 [с. 101-135], 3 [с. 373-385], 4 [с. 64-83, 92-123]

Додатковий: 5 [с. 67-95], 7 [с. 96-122], 9 [с. 143-210], 10 [с. 206-240],11 [с. 192-198], 12 [с. 53-67]

Інтернет-ресурси: 13-19

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.

Список рекомендованих джерел:

Основний: 1 [с. 38-49], 2 [с. 7-11]

Додатковий: 7 [с. 55-66]

Інтернет-ресурси: 13-19

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.

Список рекомендованих джерел:

Основний: 2 [с. 157-202]

Додатковий: 6 [с. 13-15, 28-42], 12 [с. 109-123]

Інтернет-ресурси: 13-19

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.

Список рекомендованих джерел:

Основний: 1[с. 25-31, 65-85]

Додатковий: 7 [с. 6-17, 55-96]

Інтернет-ресурси: 13

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.

Список рекомендованих джерел:

Основний: 1 [с.139-158], 2 [с. 153-157], 3 [с. 373-378, 385-427]

Додатковий: 10 [с. 206-240], 12 [с. 57-115].

Інтернет-ресурси: 13, 18-19

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.

Список рекомендованих джерел:

Основний: 2[136-144]

Додатковий: 10 [с. 220-240]

Інтернет-ресурси: 13, 18-19

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.

Список рекомендованих джерел:

Основний: 1 [с. 31-92, 101-158], 3 [с. 373-378, 385-427]

Додатковий: 5 [с. 67-95], 9 [с. 143-210], 10 [с. 206-240] 11 [с. 192-198], 12 [с. 48-86], 12 [с. 57-115]

Інтернет-ресурси: 13, 18-19

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.

Список рекомендованих джерел:

Основний: 1 [с. 31-92, 101-158], 3 [с. 373-378, 385-427], 4 [с. 64-83, 92-123]

Додатковий: 9 [с. 143-210], 10 [с. 206-240], 11 [с. 192-198], 12 [с. 48-86], 12 [с. 57-115]

Інтернет-ресурси: 13, 18-19

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 рекомендованих джерел:

Основний: 1 [113-116], 2 [с. 94-106]

Додатковий: 10 [с. 92-11]

Інтернет-ресурси: 19

5. СПИСОК РЕКОМЕНДОВАНИХ ДЖЕРЕЛ

Основний

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.*

Додатковий

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.*
6. Сайко В.Г., Амірханов Е.Д. Мережі цифрового радіозв’язку і радіодоступу нового покоління. Навчальний посібник. – К.: ДУТ, 2015. – 77 с.
7. Інформаційна безпека в середовищі безпроводових сенсорних мереж: монографія / Александер М.Б., Балабан С.М., Карпінський М.П., Райба С.А., Чиж В.М. – Тернопіль : Вид-во ТНТУ імені Івана Пулюя, 2016. – 160 с.
8. Гнатушенко, В.В. Системи супутникового та стільникового зв’язку: навч. посіб. / В.В. Гнатушенко, О.О. Дробахін, В.М. Корчинський. – Д.: РВВ ДНУ, 2012. – 80 с.
9. 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.
10. Комплексна безпека інформаційних мережевих систем. Навчальний посібник / А.Г. Микитишин, М.М. Митник, П.Д. Стухляк. – Львів, «Магнолія 2006», 2016. – 256 с.
11. Довгий С.О. Сучасні телекомунікації: Мережі, технології, безпека, економіка, регулювання. Монографія / С.О. Довгий, П.П. Воробієнко, К.Д. Гуляєв. – 2-ге вид. – К.: «Азимут Україна», 2013. – 608 с.

12. Соколов В.Ю. Безпека безпроводових і мобільних мереж : Лабораторний практикум / В. Ю. Соколов, М. Тадж-Діні / ред. перекл. О. П. Райтер. – К. : ДУТ, 2018. – 122 с.

Інтернет-ресурси

13. Продукти ESET для бізнесу. − Режим доступу: https://www.eset.com/ua/business/entry-protection-bundle/.
14. Засоби захисту інформації − Режим доступу: http://allref.com.ua/uk/skachaty/Zasobi_zahistu_informaciyi?page=7.
15. Десять правил безпеки мобільних пристроїв. − Режим доступу: https://blog.allo.ua/ua/desyat-pravil-bezpeki-mobilnih-pristroyiv_2020-01-39/.
16. Хмарна система контролю доступом. − Режим доступу: https://www.samekey.com/?lang=uk&gclid=EAIaIQobChMI84Xtg4HR8wIVweeyCh0Mrw4IEAAYASAAEgICAvD_BwE.
17. Mobile Policy Handbook [Електронний ресурс] − Режим доступу: https://www.gsma.com/latinamerica/wp-content/uploads/2019/03/GSMA_Mobile-Policy-Handbook_2019_ENG.pdf.
18. Вступ до систем виявлення вторгнень (IDS) – Home | 2021. − Режим доступу: https://uk.go-travels.com/95456-introduction-to-intrusion-detection-systems-ids-2486799-3152184.
19. Захист інформації в операційних системах, базах даних і мережах. − Режим доступу: https://ppt-online.org/482411.

**Курсивом зазначені джерела, що є в наявності в бібліотеці КНТЕУ*