Силабус освітнього компонента
Програма навчальної дисципліни

Безпека та аудит бездротових та рухомих мереж

Шифр та назва спеціальності
К4 – Управління інформаційною безпекою

Інститут
ННІ комп`ютерних наук та інформаційних технологій

Спеціалізація

Кафедра
Кібербезпеки (328)

Освітня програма
Управління інформаційною безпекою

Тип дисципліни
Вибіркова

Рівень освіти
Перший (бакалаврський)

Форма навчання
Денна

Семестр
8

Мова викладання
Українська

Викладачі, розробники

КОРОЛЬОВ Роман Володимирович

korolevrv01@ukr.net
Кандидат технічних наук, доцент, доцент кафедри кібербезпеки НТУ «ХПІ».

Кількість наукових публікацій: понад 40, з яких 1 навчальний посібник, 23 статті у закордонних виданнях та фахових виданнях України, 10 патентів на корисну модель. Провідний лектор з дисциплін: «Фізичні основи технічних засобів розвідки», «Основи стеганографічного захисту інформації», «Корпоративні мережі та системи доступу» , «Безпека та аудит бездротових та рухомих мереж», гарант освітньо-професійної програми "Управління інформаційною безпекою" першого (бакалаврського) рівня вищої освіти.

Детальніше про викладача на сайті кафедри

Загальна інформація

Анотація

Навчальна дисципліна "Безпека та аудит бездротових та рухомих мереж" є вибірковою навчальною дисципліною. Дисципліна спрямована на формування теоретичних знань та практичних умінь у сфері бездротових і мобільних технологій, інформаційної та кібернетичної безпеки та набуття відповідних компетентностей.

Мета та цілі дисципліни

Формування у студентів уміння вирішувати задачі адміністрування безпроводових і мобільних мереж і систем, застосовувати нормативно-правові, організаційні та технічні процедури при роботі бездротових і мобільних технологій.

Формат занять

Лекції, лабораторні заняття, самостійна робота, консультації. Підсумковий контроль – іспит.

Компетентності

ЗК6. Здатність до пошуку, оброблення та аналізу інформації з різних джерел.
ЗК7. Здатність використовувати інформаційні та комунікаційні технології та формувати систему інформаційно-аналітичного забезпечення підтримки прийняття управлінських рішень щодо системи управління інформаційною безпекою.
СК2. Здатність аналізувати та визначати політику та стратегії забезпечення захисту інформації.
СК3. Проектувати системи управління та захисту інформації на підприємстві установі, організації.
СК5. Здатність узагальнення вітчизняного та закордонного досвіду з питань управління інформаційною безпекою.
СК7. Здатність організовувати та проводити аналіз оточення організації установ з метою виявлення та закриття можливих каналів витоку інформації.
СК8. Здатність використовувати механізми забезпечення управління інформаційною безпекою у її визначальних сферах.
СК9. Здатність організації реагування на загрози на об'єктах критичної інфраструктури, установах та підприємствах.
СК10. Здатність забезпечувати неперервність бізнесу згідно з встановленою політикою інформаційної безпеки.
СК11. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації.

Результати навчання

РН3. Вміти за допомогою абстрактного мислення, аналізу та синтезу оцінювати результати професійної діяльності та забезпечувати її якість, бути критичним і самокритичним, наполегливим щодо поставлених завдань і взятих зобов'язань.
РН6. Впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної безпеки.
РН7. Вміти розробляти комплекс організаційних заходів щодо формування системи управління інформаційною безпекою.
РН8. Вміти використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій щодо формування системи управління інформаційної безпеки.
РН10. Вміти аналізувати виклики та загрози інформаційної безпеки об'єктів критичної інфраструктури та синтезувати інформацію щодо розроблення та реалізації стратегій та політики безпеки.
РН11. Вміти забезпечувати процеси захисту та функціонування системи управління інформаційною безпекою та захисту інформації на основі практик, навичок та знань, щодо інфраструктури кіберфізичних систем та інформаційних потоків.
РН12. Вміти використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів.
РН13. Вміти вирішувати задачі забезпечення та супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління інформаційної безпеки згідно встановленої політики безпеки в інформаційно-комунікаційних системах.
РН14. Вміти вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів та користувачів в інформаційно-комунікаційних системах згідно встановленої політики інформаційної безпеки.
РН16. Вміти реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційно-комунікаційних системах.

РН17. Вміти розв'язувати задачі управління інфораційною безпекою в інформаційно-комунікаційних системах на основі моделей управління безпекою.
РН18. Розуміти основні теоретичні поняття, застосовувати набуті практичні навички дослідження та підготовки документів, їх правильного використання в управлінській діяльності.
РН19. Вміти впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформації в інформаційно-мунікаційних системах.
РН20. Вміти аналізувати та проводити оцінку ефективності та рівня захищеності інформаційних ресурсів в інформаційно-комунікаційних системах згідно встановленої політики інформаційної безпеки.
РН21. Вміти застосовувати теорії та методи захисту для забезпечення безпеки елементів об'єктів критичної інфраструктури, кіберфізичних систем та інформаційно-комунікаційних систем.
РН22. Вміти застосовувати національні та міжнародні регулятори в сфері інформаційної безпеки щодо розслідування комп'ютерних інцидентів.

Обсяг дисципліни

Загальний обсяг дисципліни 90 год. (3 кредити ECTS): лекції – 10 год., лабораторні роботи – 20 год., самостійна робота – 60 год.

Передумови вивчення дисципліни (пререквізити)

Математичні основи криптології, Комп'ютерні мережі.

Особливості дисципліни, методи та технології навчання

В ході викладання дисципліни викладачем застосовуються пояснювально-ілюстративний (інформаційно-рецептивний) та репродуктивний методи навчання. В якості методів викладання, які направлені на активізацію та стимулювання навчально-пізнавальної діяльності здобувачів, застосовуються презентації, бесіди, індивідуальні групові проєкти, майстер-класи.

Програма навчальної дисципліни

Навчальні заняття

Лекції

Теми лекцій	Кількість годин
Тема 1. Введення в бездротові мережі. Фундамент безпечної мережі. Особливості радіомереж. Технологія широкосмугового сигналу. Стандарти бездротової мережі. Канальний рівень стандарту 802.11. Структура мережі.Сервіси канального рівня. Політика безпеки. Базові механізми захисту. Списки контролю доступу.	2
Тема 2. Безпека протоколу WEP. Протокол WPA. Безпека технології Bluetooth. Основні недоліки WEP. Слабкі вектори ініціалізації. Протокол WPA-PSK. Протокол TKIP. Стек протоколів Bluetooth. Уразливості пристроїв Bluetooth.	2
Тема 3. Безпека мережевого рівня. Атаки на користувачів WLAN. Міжмережеве екранування бездротової мережі. Топологія мережі. Вибір типу міжмережевого екрана. Налаштування міжмережевого екрана. Віртуальні приватні мережі. VPN мережевого рівня. Протокол IPv6. Основи безпеки протоколу IPv6. Хибна точка доступу. Атаки на 802.1X. Уразливості драйверів.	2

Тема 4. Захист мобільних користувачів. Виявлення атак та контроль захищеності. Контроль бездротових клієнтів. Централізоване налаштування Wi-Fi. Персональні системи виявлення атак. Виявлення бездротових атак. Приклади систем виявлення бездротових атак.	2
Тема 5. Оцінка захищеності бездротових мереж. Захист інформації в системах мобільного зв'язку. Засоби захисту в сучасних системах мобільного зв'язку. Аналіз конфігурацій. Тестування на проникнення. Засоби захисту в сучасних системах мобільного зв'язку.	2
Загальна кількість годин	**10**

Лабораторні заняття

Теми лабораторних занять	Кількість годин	Вагові коефіцієнти a
Тема 1. Розрахунок дальності роботи бездротового каналу зв'язку 802.11. Ознайомлення із стандартами IEEE 802.11 і використовуваними діапазонами частот. Визначати дальність роботи каналу зв'язку 802.11 в залежності від необхідної швидкості передачі і використовуваного частотного каналу.	5	0,1
Тема 2. Дослідження алгоритма поточного шифрування RC4. Дослідження періодичних властивостей алгоритму поточного шифрування RC4.	5	0,1
Тема 3. Дослідження періодичних властивостей алгоритму A5/1. Огляд та дослідження періодичних властивостей міні версії алгоритму потокового шифрування A5/1.	5	0,1
Тема 4. Дослідження безпеки Bluetooth. Ознайомлення з Bluetooth-стеком. Виявлення Bluetooth-пристроїв. Демонстрація атак Bluejacking, Bluesnarfing. Аналіз захисту Bluetooth LE.	5	0,1
Загальна кількість годин	**20**	$\sum_{i=1}^{n} a_i = 0{,}4$

Контрольні роботи

Теми контрольних робіт	Вагові коефіцієнти b
Тема 1. Введення в бездротові мережі. Особливості радіомереж. Технологія широкосмугового сигналу. Стандарти бездротової мережі. Канальний рівень стандарту 802.11. Структура мережі.Сервіси канального рівня.	0,2
Загалом	$\sum_{i=1}^{m} b_i = 0{,}2$

Самостійна робота

До самостійної роботи відноситься самостійне опрацювання теоретичного матеріалу

Опрацювання теоретичного матеріал

Теми для самостійного вивчення	Кількість годин
Тема 1. Основи безпеки бездротових мереж. Основні принципи безпеки бездротових мереж (CIA-тріада) та їх застосування в Wi-Fi. Архітектура бездротових мереж (WLAN, WPAN) та ключові компоненти безпеки.	6
Тема 2. Загрози та вразливості в бездротових мережах. Основні загрози бездротовим мережам (eavesdropping, man-in-the-middle) та приклади атак. Як класифікуються вразливості в бездротових мережах за типами (конфігураційні, протоколні).	6
Тема 3 Протоколи шифрування в Wi-Fi мережах. Еволюція протоколів шифрування Wi-Fi (WEP, WPA, WPA3) та їх сильні/слабкі сторони. Роль EAP (Extensible Authentication Protocol) у аутентифікації користувачів Wi-Fi.	6
Тема 4. Безпека мобільних мереж (GSM, UMTS). Ключові механізми безпеки в GSM (A3/A8 алгоритми) та їх вразливості до атак. Шифрування в UMTS (KASUMI) та методи захисту від IMSI-catching.	6
Тема 5. Безпека мереж LTE та 5G. Нові функції безпеки в 5G (network slicing, SUCI) порівняно з LTE. Протоколи аутентифікації в LTE (EPS-AKA) та ризики SS7-атак.	6
Тема 6. Методи аудиту бездротових мереж. Проводення пентестингу в бездротових мережах (використання інструментів як Aircrack-ng). Стандарти аудиту (ISO 27001, NIST) для оцінки безпеки WLAN.	6
Тема 7. Системи виявлення вторгнень у бездротових мережах. Принципи роботи WIPS (Wireless Intrusion Prevention System) та їх інтеграцію. Методи виявлення аномалій (signature-based, anomaly-based) застосовуються в мобільних мережах.	6
Тема 8. Безпека Bluetooth та NFC технологій. Вразливості Bluetooth (BlueBorne, KNOB) та методи їх пом'якшення. Механізми безпеки NFC (контактна аутентифікація) та ризики relay-атак.	6
Тема 9. Аудит безпеки IoT у бездротових мережах. Як проводити аудит безпеки IoT-пристроїв (Zigbee, Z-Wave) на вразливості? Рекомендації для сегментації мереж IoT для мінімізації ризиків.	6
Тема 10. Стандарти та регуляції безпеки бездротових мереж. Міжнародні стандарти (IEEE 802.11, 3GPP) регулюють безпеку бездротових та рухомих мереж. Роль GDPR та інших регуляцій у аудиті мобільних мереж.	6
Загальна кількість годин	**60**

Неформальна освіта

Здобувач має можливість перезарахувати окремі теми або курс шляхом: проходження професійних курсів чи тренінгів, онлайн-освіти, професійних стажувань, у сфері, що відповідає навчальним цілям дисципліни.
Для зарахування необхідно надати: сертифікат (електронний або друкований) про проходження курсу/стажування, опис програми тренінгу із зазначенням змісту тем, обсягу та тривалості..

Рекомендовані курси, тренінги, стажування

За даним компонентом врахування тем, у разі успішного завершення курсів, не передбачено.

Література, навчальні матеріали та інформаційні ресурси

Основна література

1. Про захист інформації в інформаційно-телекомунікаційних системах: Закон України від 05.07.1994 № 80/94-ВР. Дата оновлення: 31.12.2023. URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text
2. Про захист персональних даних: Закон України від 01.06.2010 № 2297-VI. Дата оновлення: 27.10.2022. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text
3. Бурячок В. Л. Основи інформаційної та кібернетичної безпеки. [Навчальний посібник]. / В. Л. Бурячок , Р. В. Киричок, П. М. Складанний – К. , 2018. – 320 с.
4. Бурячок В. Л., Соколов В. Ю. Методи забезпечення гарантоздатності і функціональної безпеки безпроводової інфраструктури на основі апаратного розділення абонентів : Монографія. Київ : КУБГ, 2019. 164 с.
5. Соколов, В. Ю. Безпека безпроводових і мобільних мереж : Навчальний посібник / В. Ю. Соколов, В. Л. Бурячок, М. М. Таджділі / ред. перекл. О. П. Райтер. — 2 вид., доп. — К. : КУБГ, 2019. — 130 с.
6. Ахрамович В.М. Курс лекцій з навчальної дисципліни «Кібербезпека банківських та комерційних структур» /В.М.Ахрамович. Державний університет телекомунікацій. – К.:ДУТ, 2019. – 163 с. іл. – Бібліограф.: 166 с.
7. Безпека електронної комерції: навч. посібн. І.М. Пістунов, Є.В., Кочура; Нац. гірн. ун–т. Дніпропетровськ: НГУ, 2014. 125 с.
8. Основи інформаційної безпеки / Андрєєв В. І. та ін. ; за ред. В. О. Хорошка. 2-е вид. Київ, 2009. 292 с.
9. ДСТУ 3396 0-96 Захист інформації. Технічний захист інформації. Основні положення. URL: https://tzi.com.ua/downloads/DSTU%203396.0-96.pdf
10. ДСТУ 3396 1-96 Захист інформації. Технічний захист інформації. Порядок проведення робіт. URL: https://tzi.com.ua/downloads/DSTU%203396.1-96.pdf
11. НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу, наказ ДСТСЗІ СБУ від 28.04.99 № 22 (Зміна № 1 наказ від 28.12.2012 № 806).
https://tzi.com.ua/downloads/2.5-004-99.pdf
12. Information Security Handbook for Network Beginners. National Center of Incident Readiness and Strategy for Cybersecurity (NISC) ver. 2.11e.
https://www.coursehero.com/file/55121963/handbook-all-engpdf/
13. Євсєєв С.П. Кібербезпека: основи кодування та криптографії/ С.П. Євсеєв, О.В. Мілов, С.Е. Остапов, О.В. Сєвєрінов. – Харків: Вид. "Новий Світ-2000", 2023. – 657 с.
https://acrobat.adobe.com/id/urn%3Aaaid%3Asc%3AEU%3A3c427761-01ab-4365-88f6-37f76ca508c5/?x_api_client_id=chrome_extension_viewer&bookmarkAcrobat=true&x_api_client_location=bookmark&filetype=application%2Fpdf&viewer%21megaVerb=group-discover
14. Технології захисту інформації./ С. Е. Остапов, С. П. Євсєєв, О.Г. Король. – Чернівці : Чернівецький національний університет, 2013. – 471 с.
http://kist.ntu.edu.ua/textPhD/tzi.pdf

Додаткова література

1. ISO/IEC 27001:2022/Amd 1:2024 Information security, cybersecurity and privacy protection – Information security management systems – Requirements URL:
https://www.iso.org/ru/contents/data/standard/08/28/82875.html
2. ISO/IEC 27002:2023 Information security, cybersecurity and privacy protection – Information security controls URL:
https://www.iso.org/ru/contents/data/standard/08/05/80585.html

3. ISO/IEC 27005:2023 Information security, cybersecurity and privacy protection – Guidance on managing information security risks. URL: https://www.iso.org/ru/contents/data/standard/08/05/80585.html.
4. Домарев В. В. Безпека інформаційних технологій. Методологія створення систем захисту. Київ, 2001. 688 с.
5. Synergy of building cybersecurity systems: monograph / S. Yevseyev, V. Ponomarenko, O. Laptiev, O. Milov and others. - Kharkiv: PC TECHNOLOGY CENTER, 2021. - 188 p. URL: https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju
6. Models of socio-cyber-physical systems security: monograph / S. Yevseiev, Yu. Khokhlachova, S. Ostapov, O.Laptiev and others. - Kharkiv: PC TECHNOLOGY CENTER, 2023. - 168 p. URL: https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju
7. Modeling of security systems for critical infrastructure facilities: monograph / S. Yevseiev, R. Hryshchuk, K. Molodetska, M. Nazarkevych and others. - Kharkiv: PC TECHNOLOGY CENTER, 2022. - 196 p. URL: https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju.

Система оцінювання

Підсумкова оцінка з освітнього компонента визначається відповідальним лектором за темами, видами занять, тощо у відповідності до силабусу і є інтегральною оцінкою результатів усіх вид навчальної діяльності здобувача вищої освіти. Підсумкова оцінка повинна відображати всі оцінки за складовими навчального процесу з урахуванням їх вагових показників k:

Поточний контроль (практичні, семінарські, лабораторні заняття), k_1	Контрольні роботи (за наявності), k_2	Індивідуальне завдання (за наявності), k_3	Підсумковий контроль (для ОК з іспитом), k_4
0,2	0,4		0,4

Сума коефіцієнтів повинна складати одиницю: $k_1 + k_2 + k_3 + k_4 = 1$. Підбір вагових коефіцієнтів підсумкової оцінки здійснює розробник курсу.
Розрахунок підсумкової оцінки проводиться за формулою:

$$О = П \cdot k_1 + K \cdot k_2 + І \cdot k_3 + Пк \cdot k_4$$

де: П – середньозважена середня оцінка за поточний контроль
І – оцінка за виконання індивідуального завдання
K – середньозважена оцінка за контрольні роботи
Пк – оцінка за підсумковий контроль

$$П = \frac{П_1 \cdot a_1 + П_2 \cdot a_2 + ... + П_n \cdot a_n}{\sum_{i=1}^{n} a_i}$$

де: a_i - ваговий коефіцієнт за кожне практичне (семінарське) або лабораторне заняття.

$$K = \frac{K_1 \cdot b_1 + K_2 \cdot b_2 + ... + K_m \cdot b_m}{\sum_{i=1}^{m} b_i}$$

де: b_i - ваговий коефіцієнт за кожну контрольну роботу.

Поточні оцінки за кожну складову (П, K, І,...) виставляються за 100-бальною шкалою згідно з положенням «Про критерії та систему оцінювання знань та вмінь і про рейтинг здобувачів вищої освіти» НТУ «ХПІ».

Шкала оцінювання

Сума балів	Національна оцінка	ECTS
90–100	Відмінно	A
82–89	Добре	B
75–81	Добре	C
64–74	Задовільно	D

Підсумкова оцінка виставляється відповідно до розрахованої О з округленням до найближчого цілого числа в більшу сторону.

60–63	Задовільно	E
35–59	Незадовільно (потрібне додаткове вивчення)	FX
1–34	Незадовільно (потрібне повторне вивчення)	F

Норми академічної етики і політика курсу

Здобувач вищої освіти повинен дотримуватися «Кодексу етики академічних взаємовідносин та доброчесності НТУ «ХПІ»: виявляти дисциплінованість, вихованість, доброзичливість, чесність, відповідальність. Конфліктні ситуації повинні відкрито обговорюватися в навчальних групах з викладачем, а при неможливості вирішення конфлікту – доводитися до відома співробітників дирекції інституту.
Нормативно-правове забезпечення впровадження принципів академічної доброчесності НТУ «ХПІ» розміщено на сайті: http://blogs.kpi.kharkov.ua/v2/nv/akademichna-dobrochesnist/

Погодження

Силабус погоджено 30.08.2025 **Завідувач кафедри**
Сергій ЄВСЕЄВ

30.08.2025 **Гарант ОП**
Роман КОРОЛЬОВ