



Силабус освітнього компонента
Програма навчальної дисципліни



Безпека та аудит бездротових та рухомих мереж

Шифр та назва спеціальності

257 – Управління інформаційною безпекою

Інститут

ННІ комп'ютерних наук та інформаційних технологій

Освітня програма

Управління інформаційною безпекою

Кафедра

Кібербезпеки (328)

Рівень освіти

Бакалавр

Тип дисципліни

Профільна підготовка, Вибіркова

Семестр

8

Мова викладання

Українська

Викладачі, розробники



КОРОЛЬОВ Роман Володимирович

korolevrv01@ukr.net

Кандидат технічних наук, доцент, доцент кафедри кібербезпеки НТУ «ХП».

Кількість наукових публікацій: понад 80, з них патентів на корисну модель 12, 1 колективна монографія, 2 навчальних посібника, 65 статті у закордонних виданнях та фахових виданнях України, з них 5 у наукометричній базі Scopus. Провідний лектор з дисциплін: «Бездротова та мобільна безпека», «Основи стеганографії», «Бізнес інтеллідженс», «Фізичні основи технічних засобів розвідки» у студентів бакалавріата та магістратури.

[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 умінь 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 роботи, самостійна робота, консультації. Підсумковий контроль – іспит.

Компетентності

КЗ-6. Здатність до пошуку, оброблення та аналізу інформації з різних джерел.

КЗ-7. Здатність використовувати інформаційні та комунікаційні технології та формувати систему інформаційно-аналітичного забезпечення підтримки прийняття управлінських рішень щодо системи управління інформаційною безпекою.

ФК-2. Здатність аналізувати та визначати політику та стратегії забезпечення захисту інформації.

ФК-3. Проектувати системи управління та захисту інформації на підприємстві установі, організації.

ФК-5. Здатність узагальнення вітчизняного та закордонного досвіду з питань управління інформаційною безпекою.

ФК-7. Здатність організовувати та проводити аналіз оточення організації установ з метою виявлення та закриття можливих каналів витоку інформації.

ФК-8. Здатність використовувати механізми забезпечення управління інформаційною безпекою у її визначальних сферах.

ФК-9. Здатність організації реагування на загрози на об'єктах критичної інфраструктури, установах та підприємствах.

ФК-10. Здатність забезпечувати неперервність бізнесу згідно з встановленою політикою інформаційної безпеки.

ФК-11. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації.

Результати навчання

ПРН-3. 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.

ПРН-6. Впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної безпеки.

ПРН-7. Вміти розробляти комплекс організаційних заходів щодо формування системи управління інформаційною безпекою.

ПРН-8. Вміти використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій щодо формування системи управління інформаційної безпеки.

ПРН-10. Вміти аналізувати виклики та загрози інформаційної безпеки об'єктів критичної інфраструктури та синтезувати інформацію щодо розроблення та реалізації стратегій та політики безпеки.

ПРН-11. 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.

ПРН-12. Вміти використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів.

ПРН-13. Вміти вирішувати задачі забезпечення та супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління інформаційної безпеки згідно встановленої політики безпеки в інформаційно-комунікаційних системах.

ПРН-14. Вміти вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів та користувачів в інформаційно-комунікаційних системах згідно встановленої політики інформаційної безпеки.

ПРН-16. Вміти реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційно-комунікаційних системах.

ПРН-17. Вміти розв'язувати задачі управління інформаційною безпекою в інформаційно-комунікаційних системах на основі моделей управління безпекою.

ПРН-18. Розуміти основні теоретичні поняття, застосовувати набуті практичні навички дослідження та підготовки документів, їх правильного використання в управлінській діяльності.

ПРН-19. Вміти впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформації в інформаційно-комунікаційних системах.

ПРН-20. Вміти аналізувати та проводити оцінку ефективності та рівня захищеності інформаційних ресурсів в інформаційно-комунікаційних системах згідно встановленої політики інформаційної безпеки.

ПРН-21. Вміти застосовувати теорії та методи захисту для забезпечення безпеки елементів об'єктів критичної інфраструктури, кіберфізичних систем та інформаційно-комунікаційних систем.

ПРН-22. 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 – 24 год., лабораторні роботи – 12 год., самостійна робота – 54 год.

Передумови вивчення дисципліни (пререквізити)

Математичні основи криптології та криптоаналіз.

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 проекти, майстер-класи.

Програма навчальної дисципліни

Теми лекційних занять

Тема 1. Введення в бездротові мережі.

Особливості радіомереж. Технологія широкосмугового сигналу. Стандарти бездротової мережі. Канальний рівень стандарту 802.11. Структура мережі. Сервіси канального рівня.

Тема 2. Фундамент безпечної мережі.

Політика безпеки. Базові механізми захисту. Списки контролю доступу.

Тема 3. Безпека протокола WEP.

Основні недоліки WEP. Слабкі вектори ініціалізації.

Тема 4. Протокол WPA.

Протокол WPA-PSK. Протокол TKIP.

Тема 5. Безпека технології Bluetooth.

Стек протоколів Bluetooth. Уразливості пристроїв Bluetooth.

Тема 6. Безпека мережевого рівня.

Міжмережеве екранування бездротової мережі. Топологія мережі. Вибір типу міжмережевого екрана. Налаштування міжмережевого екрана. Віртуальні приватні мережі. VPN мережевого рівня. Протокол IPv6. Основи безпеки протокола IPv6.

Тема 7. Атаки на користувачів WLAN.

Хибна точка доступу. Атаки на 802.1X. Уразливості драйверів.

Тема 8. Захист мобільних користувачів.

Контроль бездротових клієнтів. Централізоване налаштування Wi-Fi. Персональні системи виявлення атак.

Тема 9. Виявлення атак та контроль захищеності.

Виявлення бездротових атак. Приклади систем виявлення бездротових атак.

Тема 10. Оцінка захищеності бездротових мереж.

Аналіз конфігурацій. Тестування на проникнення.

Тема 11. Захист інформації в системах мобільного зв'язку.

Засоби захисту в сучасних системах мобільного зв'язку.

Теми практичних занять

Практичні роботи в рамках дисципліни не передбачені.

Теми лабораторних робіт

Тема 1. Встановлення Kali Linux на комп'ютер або віртуальну машину (флеш носій або зовнішній диск).

Тема 2. Дослідження стійкості точок доступу бездротової мережі Wi-Fi.

Тема 3. Використання утиліт Kali Linux для створення словників.

Тема 4. Використання сканера безпеки Nmap та Zmap на Kali Linux.

Самостійна робота

Самостійна робота студента є однією з форм організації навчання, основною формою оволодіння навчальним матеріалом у вільний від аудиторних навчальних занять час. Під час самостійної роботи студенти вивчають лекційний матеріал, готуються до лабораторних робіт, контрольних робіт, заліків та іспитів. Студентам також рекомендуються додаткові матеріали (відео, статті) для самостійного вивчення та аналізу.

Неформальна освіта

В рамках неформальної освіти згідно відповідного Положення (<http://surl.li/pxssv>), освітня компонента або її окремі теми можуть бути враховано у разі самостійного проходження професійних курсів/тренінгів, отримання громадянської освіти, онлайн освіти, професійного стажування тощо.

Зокрема, окремі теми даної компоненти можуть бути враховано у разі успішного завершення таких курсів CISCO:

Network Support and Security

<https://www.netacad.com/catalogs/learn?category=course>.

Література та навчальні матеріали

Основна література

1. Бурячок В. Л. Основи інформаційної та кібернетичної безпеки. [Навчальний посібник]. / В. Л. Бурячок, Р. В. Киричок, П. М. Складанний – К., 2018. – 320 с.
https://elibrary.kubg.edu.ua/id/eprint/27370/1/V_Buriachok_Posibnik_2019_FITU.pdf
2. 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.
https://elibrary.kubg.edu.ua/id/eprint/28225/1/V_Buriachok_V_Sokolov_WMS.pdf
3. Соколов, В. Ю. Безпека безпроводових і мобільних мереж : Навчальний посібник / В. Ю. Соколов, В. Л. Бурячок, М. М. Тадждіні / ред. перекл. О. П. Райтер. — 2 вид., доп. — К. : КУБГ, 2019. — 130 с.
https://elibrary.kubg.edu.ua/id/eprint/27294/1/V_Sokolov_V_Buriachok_M_Taj_Dini_WMS_2.pdf
4. 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.
<https://b.twirpx.link/file/3149823/>
5. Безпека електронної комерції: навч. посібн. І.М. Пістунов, Є.В., Кочура; Нац. гірн. ун-т. Дніпропетровськ: НГУ, 2014. 125 с.
http://pistunovi.inf.ua/6_E_K.pdf
6. Дудікевич, В. Б. Основи інформаційної безпеки : навч. пос. / Дудікевич В. Б., Хорошко В. О., Яремчук Ю. Є. – Вінниця : ВНТУ, 2018. – 316 с.
https://pdf.lib.vntu.edu.ua/books/IRVC/Dudikevich_2018_316.pdf.

Додаткова література

7. 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>.

8. Домарев В. В. Безпека інформаційних технологій. Методологія створення систем захисту. Київ, 2001. 688 с.

http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?I21DBN=LINK&P21DBN=UJRN&Z21ID=&S21REF=10&S21CNR=20&S21STN=1&S21FMT=ASP_meta&C21COM=S&S21P03=FILE=&S21STR=Zi_2014_16_2_10

9. Synergy of building cybersecurity systems: monograph / S. Yevseiev, V. Ponomarenko, O. Laptiev, O. Milov and others. – Kharkiv: PC TECHNOLOGY CENTER, 2021. – 188 p.

<https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju>

10. 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.

<https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju>

11. 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.

<https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju>

Система оцінювання

Критерії оцінювання успішності студента та розподіл балів

Бали нараховуються за наступним співвідношенням:

- лабораторні роботи: 40% семестрової оцінки;
- самостійна робота: 10% семестрової оцінки;
- контрольна робота: 10% семестрової оцінки;
- іспит: 40% семестрової оцінки.

Шкала оцінювання

Сума балів	Національна оцінка	ECTS
90–100	Відмінно	A
82–89	Добре	B
75–81	Добре	C
64–74	Задовільно	D
60–63	Задовільно	E
35–59	Незадовільно (потрібне додаткове вивчення)	FX
1–34	Незадовільно (потрібне повторне вивчення)	F

Норми академічної етики і політика курсу

Студент 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

28.08.2024



Завідувач кафедри
Сергій ЄВСЕЄВ

28.08.2024



Гарант ОП
Роман КОРОЛЬОВ