Силабус освітнього компонента
Програма навчальної дисципліни

Інформаційно-комунікаційні системи у сфері національної безпеки

Шифр та назва спеціальності
256 – Національна безпека (за окремими сферами забезпечення і видами діяльності)

Інститут
ННІ комп`ютерних наук та інформаційних технологій

Освітня програма
Національна безпека у сфері кіберзахисту

Кафедра
Кібербезпеки (328)

Рівень освіти
Бакалавр

Тип дисципліни
Спеціальна (фахова), Обов'язкова

Семестр
7

Мова викладання
Українська

Викладачі, розробники

КОРОЛЬОВ Роман Володимирович

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

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 інтелліджанс» , «Фізичні основи технічних засобів розвідки» у студентів бакалавріата та магістратури.

Детальніше про викладача на сайті кафедри

ПОГАСІЙ Сергій Сергійович

Serhii.Pohasii@khpi.edu.ua
Кандидат економічних наук, доцент, доцент кафедри кібербезпеки НТУ «ХПІ».

Кількість наукових публікацій: понад 95, з них патентів на корисну модель 2, 6 монографій, з яких 4 колективних монографій, 4 навчальних посібників, з яких 4 з грифом Міністерства освіти і науки України, 65 статті у закордонних виданнях та фахових виданнях України, з них 11 у наукометричній базі Scopus. Провідний лектор з дисциплін: «Аналогові та цифрові електронні пристрої», «Інтернет речей та сервісів», «Безпека хмарних технологій», «Основи побудови та захисту сучасних операційних систем», «Моделювання систем критичної інфраструктури», «Основи побудови та захисту мікропроцесорних систем», «Безпека смарт-технологій та Інтернет-речей»,

«Інформаційно-комунікаційні системи у сфері національної безпеки» у студентів бакалавріата та магістратури, Розділ «Інформаційна безпека хмарних сервісів», «Сучасні методи захисту соціо-кіберфізичних систем», «Моделювання механізмів кібербезпеки» для аспірантів.
Детальніше про викладача на сайті кафедри

Загальна інформація

Анотація

Навчальна дисципліна "Інформаційно-комунікаційні системи у сфері національної безпеки" є обов'язковою навчальною дисципліною. Навчальна дисципліна є теоретичною основою сукупності знань та вмінь, що формують профіль фахівця в області кібербезпеки. На базі здобутих знань та умінь фахівець зможе вирішувати професійні задачі, що базуються на сучасних технологіях та методах захисту інформації у сучасних інформаційно-комунікаційних системах та мережах.

Мета та цілі дисципліни

Метою навчальної дисципліни “Інформаційно-комунікаційні системи у сфері національної безпеки” є навчання студентів принципам побудови комплексних систем захисту інформації для формування контуру безпеки бізнес-процесів в інформаційно-комунікаційних системах на основі Інтернет-технологій та застосунків. Результатами вивчення даної дисципліни є придбання навичок з нейтралізації типових мережевих загроз, використання протоколу SNMP для захисту мережі, захисту від шкідливого програмного забезпечення та захист електронної пошти та веб-трафіку.

Формат занять

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

Компетентності

КЗ–1. Здатність реалізувати свої права і обов’язки як члена суспільства, усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого (безпечного) розвитку, верховенства права, прав і свобод людини і громадянина в Україні.
КЗ–7. Здатність до пошуку, оброблення та аналізу інформації з різних джерел.
КЗ–8. Здатність використовувати інформаційні та комунікаційні технології і на цій основі формувати ефективну систему інформаційно-аналітичного забезпечення підтримки прийняття управлінських рішень щодо запобігання, протидії та нейтралізації загроз національній безпеці.
ФК–1. Здатність використовувати безпекові режими під час виконання службових обов’язків.
ФК–4. Здатність демонструвати та застосовувати знання з основ теорії національної безпеки.
ФК–6. Здатність використовувати іноземну мову для отримання додаткових знань і умінь з питань національної безпеки, взаємодіяти з іноземними партнерами.
ФК–8. Здатність використовувати механізми забезпечення національної безпеки у її визначальних сферах.
ФК–13. Здатність оцінювати вплив глобальних проблем і трансформацій геополітичного та геоекономічного простору на національну безпеку.

Результати навчання

ПРН–1. Вміти реалізовувати свої права і обов’язки як члена суспільства, усвідомлювати цінності громадянського суспільства (вільного демократичного) та необхідність його сталого (безпечного) розвитку, верховенства права, прав і свобод людини і громадянина в Україні.
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–4. Вільно спілкуватися державною мовою.
ПРН–5. Вільно спілкуватися іноземною мовою у межах потреби своєї професійної діяльності.

ПРН–7. Вміти виявляти, ставити та вирішувати професійні завдання, вміти узагальнювати отримані результати, обробляти та аналізувати інформацію з різних джерел, оформлювати і презентувати результати досліджень відповідно до вимог.
ПРН–8. Вміти використовувати інформаційні та комунікаційні технології і на цій основі формувати ефективні системи інформаційно-аналітичного забезпечення підтримки прийняття рішень щодо запобігання, протидії та нейтралізації загроз національній безпеки.
ПРН–9. Вміти використовувати безпекові режими під час виконання службових обов'язків.
ПРН–10. Вміти аналізувати виклики та загрози національній безпеці за напрямами професійної діяльності та синтезувати інформацію щодо розроблення та реалізації стратегій у визначальних сферах національної безпеки (політичній, економічній, соціальній, гуманітарній).
ПРН–12. Вміти застосовувати знання з основ теорії національної безпеки, зокрема: оцінювати обстановку, рівень викликів та загроз національній безпеці.
ПРН–14. Вміти читати й розуміти фахову іншомовну літературу, використовуючи її у соціальній і професійній сферах, а також демонструвати культуру мислення та виявляти навички щодо організації культурного діалогу з іноземними партнерами на рівні, необхідному для професійної діяльності.
ПРН-16. Використовувати у професійній діяльності окремі елементи механізму впливу та взаємодії у процесі забезпечення окремих складових національної безпеки.
ПРН–17. Вміти використовувати отримані знання щодо безпекової складової зовнішньої політики України та інших держав.
ПРН–19. Вміти використовувати у професійній діяльності методи та інструменти організації соціальної взаємодії, співробітництва та розв'язання конфліктів у сфері професійної діяльності, практичні навички, тактику та прийоми, роботи з людьми в інтересах службової діяльності: працювати у команді з позицій лідера, радника (консультанта), помічника, планувати використання часу та визначати стимули і бар'єри ефективної роботи, здійснювати розподіл (делегування) функцій, повноважень і відповідальності між виконавцями.
ПРН–21. Вміти оцінювати вплив глобальних проблем і трансформацій геополітичного та геоекономічного простору на національну безпеку, здійснювати моніторинг зовнішньої та внутрішньої політики держави у контексті забезпечення національної безпеки та готувати пропозиції щодо підвищення її ефективності.

Обсяг дисципліни

Загальний обсяг дисципліни 120 год. (4 кредити ECTS): лекції – 16 год., лабораторні роботи – 32 год., самостійна робота – 72 год.

Передумови вивчення дисципліни (пререквізити)

Дисципліна базується на дисциплінах «Основи інформаційної безпеки», «Програмування», «Internet-технології та кібергігієна».

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

Теми лекційних занять

Тема 1. Сучасні загрози мережевої безпеки.
Тема 2. Забезпечення безпеки мережевих пристроїв.
Тема 3. Автентифікація, авторизація та облік.
Тема 4. Впровадження технологій брандмауера.
Тема 5. Впровадження системи запобігання вторгнень.
Тема 6. Забезпечення безпеки локальної мережі (LAN).
Тема 7. Криптографічні системи захисту інформації.

Тема 8. Впровадження віртуальних приватних мереж (VPN).
Тема 9. Впровадження багатофункціонального пристрою захисту Cisco Adaptive Security Appliance (ASA).
Тема 10. Управління безпечної мережею.

Теми практичних занять

Практичні роботи в рамках дисципліни не передбачені.

Теми лабораторних робіт

Тема 1. Соціальна інженерія. Вивчення мережевих атак, а також інструменти для аудиту безпеки і проведення атак.
Тема 2. Захист маршрутизатора для адміністративного доступу
Тема 3. Захист адміністративного доступу за допомогою AAA і RADIUS.
Тема 4. Налаштування зональних міжмережевих екранів.
Тема 5. Налаштування системи запобігання вторгнень (IPS).

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

Література та навчальні матеріали

Основна література

1. Технології захисту інформації [Електронний ресурс] : підручник для студ. 122 «Комп'ютерні науки», спеціалізацій «Інформаційні технології моніторингу довкілля», «Геометричне моделювання в інформаційних системах» / Ю. А. Тарнавський; КПІ ім. Ігоря Сікорського. – Електронні текстові дані (1 файл: 2,04 Мбайт). – Київ : КПІ ім. Ігоря Сікорського, 2018. – 162 с. https://ela.kpi.ua/server/api/core/bitstreams/c50a89f5-ef09-4821-b7d6-f402882f2bd4/content
2. С. П. Євсеєв. Технології захисту інформації / С. Е. Остапов, С. П. Євсеєв, О. Г.Король. – Чернівці. – Видавничий дом "Родовід", 2014. – 428 с.
http://kist.ntu.edu.ua/textPhD/tzi.pdf
3. Швачич Г.Г., Толстой В.В., Петречук Л.М., Іващенко Ю.С., Гуляєва О.А., Соболенко О.В. Сучасні інформаційно-комунікаційні технології: Навчальний посібник. – Дніпро: НМетАУ, 2017. –230 с.
https://nmetau.edu.ua/file/ikt_tutor.pdf
5. Коробейнікова Т.І., Захарченко С.М. Технології захисту локальних мереж на основі обладнання CISCO. Львів : Вид-во Львів. політехніки, 2021. 232 с.
https://vlp.com.ua/node/20266

Додаткова література

6. Askoxylakis I., Ioannidis S., Katsikas S.K., Meadows C. (eds.) Computer Security -ESORICS 2016, Part I
https://link.springer.com/book/10.1007/978-3-319-45744-4
7. Б. Ю. Жураковський, І.О. Зенів Комп'ютерні мережі. Частина 1. [Електронний ресурс]: навч. посіб. /; КПІ ім. Ігоря Сікорського. – Електронні текстові дані(1 файл: 8,6 Мбайт). Київ : КПІ ім. Ігоря Сікорського, 2020. 336 с.

https://ela.kpi.ua/server/api/core/bitstreams/c4ecfaa7-73d5-498c-a63a-513137ee0aba/content
8. Computer Networks / ред.: P. Gaj, M. Sawicki, A. Kwiecień. Cham : Springer International Publishing, 2019. URL: https://doi.org/10.1007/978-3-030-21952- 9 (дата звернення: 29.11.2023).
9. Куперштейн , Л., Кренцін, М., Дудатьєв, А. і Каплун, В. Аналіз проблем безпеки піринговых мереж // Інформаційні технології та комп'ютерна інженерія. 54, 2 (Чер 2022), 5–14. DOI:https://doi.org/10.31649/1999-9941-2022-54-2-5-1
10. Куперштейн , Л., Кренцін, М. Аналіз тенденцій розвитку піринговых мереж // Вісник ХНУ. Технічні науки. №299(4), 2021. С. 25-29
http://journals.khnu.km.ua/vestnik/wp-content/uploads/2021/11/299-text_2021_4_t.pdf

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 — Андрій ТКАЧОВ