Силабус освітнього компонента
Програма навчальної дисципліни

Основи кібербезпеки

Шифр та назва спеціальності
113 – Прикладна математика

Інститут
ННІ Комп`ютерних наук та інформаційних технологій

Освітня програма
Інтелектуальний аналіз даних

Кафедра
Кібербезпеки

Рівень освіти
Бакалавр

Тип дисципліни
Загальна, Вибіркова

Семестр
6

Мова викладання
Українська

Викладачі, розробники

Євсеєв Сергій Петрович
serhii.yevseiev@khpi.edu.ua
Доктор технічних наук, професор, завідувач кафедри кібербезпеки НТУ «ХПІ».

Кількість наукових публікацій: понад 350, з них патентів на корисну модель 42, 17 монографій, з яких 9 колективних монографій, 31 навчальний посібник, з яких 4 з грифом Міністерства освіти і науки України, 163 статті у закордонних виданнях та фахових виданнях України, з них 61 у наукометричній базі Scopus. Провідний лектор з дисциплін: «Менеджмент інформаційної безпеки», «Введення в мережі», «Безпека банківських систем» , «Гібридні війни та національна безпека», «Аудит та моніторинг корпоративних мереж», «Blockchain: основи та приклади застосування», «Основи смарт-контрактів», «Основи кібербезпеки» у студентів бакалавріата та магістратури, Розділ «Методи і технології моніторингу та аудиту інформаційної безпеки», «Методи побудови постквантових криптосистем», «Новітні технології забезпечення кібербезпеки на основі технології блокчейн» для аспірантів
Детальніше про викладача на сайті кафедри

Загальна інформація

Анотація

Навчальна дисципліна "Основи кібербезпеки" є вибіркова навчальною дисципліною. Вивчення дисципліни спрямовано на оволодіння необхідними базовими поняттями та правилами безпечної поведінки в мережі, ознайомлення студентів з принципами побудови систем захисту інформації, ознайомлення з основними механізмами послуг безпеки, вивчення менеджменту інформаційної безпеки, навчання студентів основам аудиту інформаційної безпеки, а також вивчення студентами спеціальних механізмів кіберзахисту.

Мета та цілі дисципліни

Навчання студентів принципам побудови систем захисту інформації, дослідженню та використанню сучасних процедур забезпечення надання основних послуг безпеки інформації в кіберпросторі, проведення аудиту поточного стану інформаційної безпеки.

Формат занять

Лекції, практичні заняття, індивідуальне завдання, самостійна робота, консультації. Підсумковий контроль – залік.

Компетентності

ЗК 1. Здатність учитися й оволодівати сучасними знаннями.
ЗК 6. Здатність до абстрактного мислення, аналізу і синтезу.
ЗК 8. Знання і розуміння предметної області та розуміння професійної діяльності.
ЗК 12. Визначеність і наполегливість щодо поставлених завдань і взятих обов'язків.
СК 7. Здатність розв'язувати професійні задачі за допомогою комп'ютерної техніки, комп'ютерних мереж та Інтернету, в середовищі сучасних операційних систем, із використанням стандартних офісних додатків.
СК 8. Здатність експлуатувати та обслуговувати програмне забезпечення автоматизованих та інформаційних систем різного призначення.
СК 9. Здатність використовувати сучасні технології програмування та тестування програмного забезпечення.

Результати навчання

РН 11. Вміти застосовувати сучасні технології програмування та розроблення програмного забезпечення, програмної реалізації чисельних і символьних алгоритмів.
РН 16. Демонструвати навички взаємодії з іншими людьми, уміння працювати в команді.
РН 24. Вміти застосовувати існуючі та розробляти нові алгоритми і програмні засоби обробки даних вимірювань та спостережень, текстів, сигналів та зображень.
РН 25. Вміти застосовувати сучасні інформаційні технології та програмне забезпечення для обробки великих масивів даних на основі розподілених і хмарних сервісів.

Обсяг дисципліни

Загальний обсяг дисципліни 90 год. (3 кредити ECTS): лекції – 28 год., практичні заняття – 16 год., самостійна робота – 46 год.

Передумови вивчення дисципліни (пререквізити)

«Математичний аналіз», «Лінійна алгебра», «Аналітична геометрія», «Алгоритмізація та програмування», «Дискретні структури і структури даних».

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

Cisco Networking Academy:
Тема 1. Кібербезпека - світ фахівців і злочинців.
Світ кібербезпеки. Кіберзлочинці проти фахівців з кібербезпеки. Загальні загрози. Розповсюдження загроз кібербезпеки. Підготовка більшої кількості спеціалістів.
Cisco Networking Academy:
Тема 2. Куб кібербезпеки.
Тріада КЦД (CIA). Стани даних. Контрзаходи кібербезпеки. Структура управління ІТ-безпекою.
Cisco Networking Academy:
Тема 3. Кібербезпека – загрози, вразливості та атак.

Шкідливе програмне забезпечення та зловмисний код. Шахрайство. Атаки.
Cisco Networking Academy:
Тема 4. Мистецтво захисту таємниць.
Криптографія. Контроль доступу. Приховування даних.
Cisco Networking Academy:
Тема 5. Мистецтво забезпечення цілісності даних.
Типи засобів контролю цілісності даних. Цифрові підписи. Сертифікати. Забезпечення цілісності баз даних.
Cisco Networking Academy:
Тема 6. Концепція п’яти дев’яток.
Висока доступність. Заходи для поліпшення доступності. Реакція на інцидент. Аварійне відновлення.
Cisco Networking Academy:
Тема 7. Захист домену кібербезпеки.
Захист систем та пристроїв. Укріплення захисту серверів. Укріплення захисту мережі. Фізична безпека.
Cisco Networking Academy:
Тема 8. Як стати спеціалістом з кібербезпеки.
Домени кібербезпеки. Розуміння етики роботи у кібербезпеці. Наступний крок.

Теми практичних занять

Cisco Networking Academy:
Тема 1. Аутентифікація, авторизація та облік.
Cisco Networking Academy:
Тема 2. Встановити віртуальну машину на персональний комп'ютер.
Cisco Networking Academy:
Тема 3. Виявлення загроз і вразливостей.
Cisco Networking Academy:
Тема 4. Використання стеганографії.
Cisco Networking Academy:
Тема 5. Злам паролів.
Cisco Networking Academy:
Тема 6. Використання цифрових підписів.
Cisco Networking Academy:
Тема 7. Віддалений доступ.
Cisco Networking Academy:
Тема 8. Захист Linux систем.

Теми лабораторних робіт

Лабораторні роботи в рамках дисципліни не передбачені.

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, виконують індивідуальне завдання, готуються до лабораторних робіт, контрольних робіт та заліку.

Література та навчальні матеріали

Основна література

1. Євсеєв С.П. Кібербезпека: сучасні технології захисту. / Євсеєв С. П, Остапов С. Е., Король О. Г. // Навчальний посібник для студентів вищих навчальних закладів. Львів: “Новий Світ – 2000”, 2019. – 678.
http://ns2000.com.ua/wp-content/uploads/2019/11/Kiberbezpeka-suchasni-tekhnolohii-zakhystu.pdf

2. Кібербезпека в сучасному світі : матеріали ІІІ Всеукраїнської науково-практичної конференції (м. Одеса, 19 листопада 2021 р.) / за ред. О. В. Дикого ;уклад.: С. А. Горбаченко, Н. І. Логінова. – Одеса, 2020. – 148 с.
http://dspace.onua.edu.ua/handle/11300/15973
3. Лісовська Ю. Кібербезпека. Ризики та заходи. – К.: Кондор, 2019. – 272 с.
http://dcmaup.com.ua/assets/files/kiberbezpeka.pdf
4. 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
5. 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
6. 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

Додаткова література

7. Доктрина інформаційної безпеки України, затверджено Указом Президента України редакція від 30.12.2021 № 47/2017. [Електронний ресурс].
https://zakon.rada.gov.ua/laws/show/47/2017#Text.
8. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України", затверджено Указом Президента України редакція від 26.08.2021 № 447/2021).
https://zakon.rada.gov.ua/laws/show/447/2021#Text
9. ISO/IEC 15408-1:2022 Information security, cybersecurity and privacy protection – Evaluation criteria for IT security – Part 1: Introduction and general model.
URL: https://www.iso.org/search.html?q=15408-1.
10. ISO/IEC 15408-2:2022 Information security, cybersecurity and privacy protection – Evaluation criteria for IT security – Part 2: Security functional components. URL:
https://www.iso.org/search.html?q=15408-2&hPP=10&idx=all_en&p=0.
11. ISO/IEC 15408-3:2022 Information security, cybersecurity and privacy protection – Evaluation criteria for IT security – Part 3: Security assurance components.
URL: https://www.iso.org/search.html?q=15408-3&hPP=10&idx=all_en&p=0.
12. ISO/IEC 31010:2019 Risk management . URL:
https://www.iso.org/ru/contents/data/standard/07/21/72140.html
13. ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection – Information security management systems – Requirements URL:
https://www.iso.org/ru/contents/data/standard/08/28/82875.html Ризик-менеджмент
14. ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection – Information security controls URL:
https://www.iso.org/ru/contents/data/standard/08/05/80585.html
15. ISO/IEC 27003:2017 Information technology – Security techniques – Information security management systems – Guidance URL:
https://www.iso.org/ru/contents/data/standard/06/34/63417.html
16. ISO/IEC 27005:2022 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
17. ISO/IEC 27032:2023 Cybersecurity – Guidelines for Internet security. URL:
https://www.iso.org/ru/contents/data/standard/07/60/76070.html.

Система оцінювання

Критерії оцінювання успішності студента та розподіл балів

Бали нараховуються за наступним співвідношенням:
•практичні роботи: 30% семестрової оцінки;
•самостійна робота: 10% семестрової оцінки;
•контрольна робота: 10% семестрової оцінки;
•індивідуальне завдання: 20% семестрової оцінки;
•залік: 30% 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

Дата погодження, підпис
28.08.2023

Завідувач кафедри
Сергій ЄВСЕЄВ

Дата погодження, підпис
31.08.2023 р.

Гарант ОП
Олена АХІЄЗЕР