Силабус освітнього компонента
Програма навчальної дисципліни

Основи кібербезпеки

Шифр та назва спеціальності
122 Комп'ютерні науки

Інститут
ННІ комп`ютерних наук та інформаційних технологій (320)

Освітня програма
Комп'ютерні науки. Штучний інтелект та управління проєктами

Кафедра
Кібербезпеки (328)

Рівень освіти
Бакалавр

Тип дисципліни
Спеціальна (фахова),Обов`язкова

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 обов`язковою 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, лабораторні роботи, самостійна робота, консультації. Підсумковий контроль – іспит.

Компетентності

ЗК1. Здатність до абстрактного мислення, аналізу та синтезу.
ЗК2. Здатність застосовувати знання у практичних ситуаціях.
ЗК3. Знання та розуміння предметної області та розуміння професійної діяльності.
ЗК4. Здатність спілкуватися державною мовою як усно, так і письмово.
ЗК6. Здатність вчитися й оволодівати сучасними знаннями.
ЗК7. Здатність до пошуку, оброблення та аналізу інформації з різних джерел.
ЗК8. Здатність генерувати нові ідеї (креативність).
ЗК10. Здатність бути критичним і самокритичним
ЗК11. Здатність приймати обґрунтовані рішення.
ЗК13. Здатність діяти на основі етичних міркувань.
ЗК14. Здатність реалізувати свої права і обов’язки як члена суспільства, усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні.
СК14. Здатність застосовувати методи та засоби забезпечення інформаційної безпеки, розробляти й експлуатувати спеціальне програмне забезпечення захисту інформаційних ресурсів об’єктів критичної інформаційної інфраструктури.

Результати навчання

РН1 Застосовувати знання основних форм і законів абстрактно-логіч-ного мислення, основ методології наукового пізнання, форм і ме-тодів вилучення, аналізу, обробки та синтезу інформації в предме-тній області комп'ютерних наук .
РН15 Розуміти концепцію інформаційної безпеки, принципи безпечного проєктування програмного забезпечення, забезпечувати безпеку комп’ютерних мереж в умовах неповноти та невизначеності вихідних даних.

Обсяг дисципліни

Загальний обсяг дисципліни 90 год. (3 кредити ECTS): лекції – 16 год., лабораторні роботи – 32 год., самостійна робота – 42 год.

Передумови вивчення дисципліни (пререквізити)

Вища математика, Комп'ютерні системи, мережі та комунікації, Алгоритми та 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 IT-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

Практичні роботи в рамках дисципліни не передбачені.

Теми лабораторних робіт

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.

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 та іспиту.

Література та навчальні матеріали

Основна література

1. Євсеєв С.П, Остапов С.Е., Король О.Г. Кібербезпека: сучасні технології захисту. Навчальний посібник для студентів вищих навчальних закладів. Львів: "Новий Світ- 2000", 2019. – 678.
2. Р. В. Грищук, та Ю. Г. Даник. Основи кібернетичної безпеки: Монографія /; за заг. ред. Ю. Г. Данника. Житомир: ЖНАЕУ, 2016.
3. І. С. Іванченко, В. О. Хорошко, Ю. Е.Хохлачова, та Д. В. Чирков під заг. ред. проф. В. О. Хорошка, "Забезпечення інформаційної безпеки держави", К: ПВП "Задруга", 2013.
4. Synergy of building cybersecurity systems: monograph / S. Yevseiev, V. Ponomarenko, O. Laptiev, O. Milov and others. – Kharkiv: PC TECHNOLOGY CENTER, 2021. – 188 p.
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.
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.

Додаткова література

1. Баранов А.А., Інтернет речей: теоретико-методологічні основи правового регулювання. Том I. Сфери застосування, ризики і бар'єри, проблеми правового регулювання, ISBN: 978-966-937-513-1, 2018, 344с.
2. Доктрина інформаційної безпеки України, затверджено Указом Президента України від 25 лютого 2017 року № 47/2017. [Електронний ресурс]. Доступно: http://zakon3.rada.gov.ua/laws/show/47/2017/paran2#n2.
3. Стратегія кібербезпеки України" (Введено в дію Указом Президента України від 15 березня 2016 року №96/2016).
4. 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.
5. 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.
6. 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.
7. ISO/IEC 31010:2019 Risk management . URL: https://www.iso.org/ru/contents/data/standard/07/21/72140.html
8. 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
9. 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
10. 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
11. 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
12. 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:
•лабораторні роботи: 30% семестрової оцінки;
•самостійна робота: 10% семестрової оцінки;
•контрольна робота: 20% 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

27.08.2024

Завідувач кафедри
Сергій ЄВСЕЄВ

27.08.2024

Гарант ОП
Марина ГРИНЧЕНКО